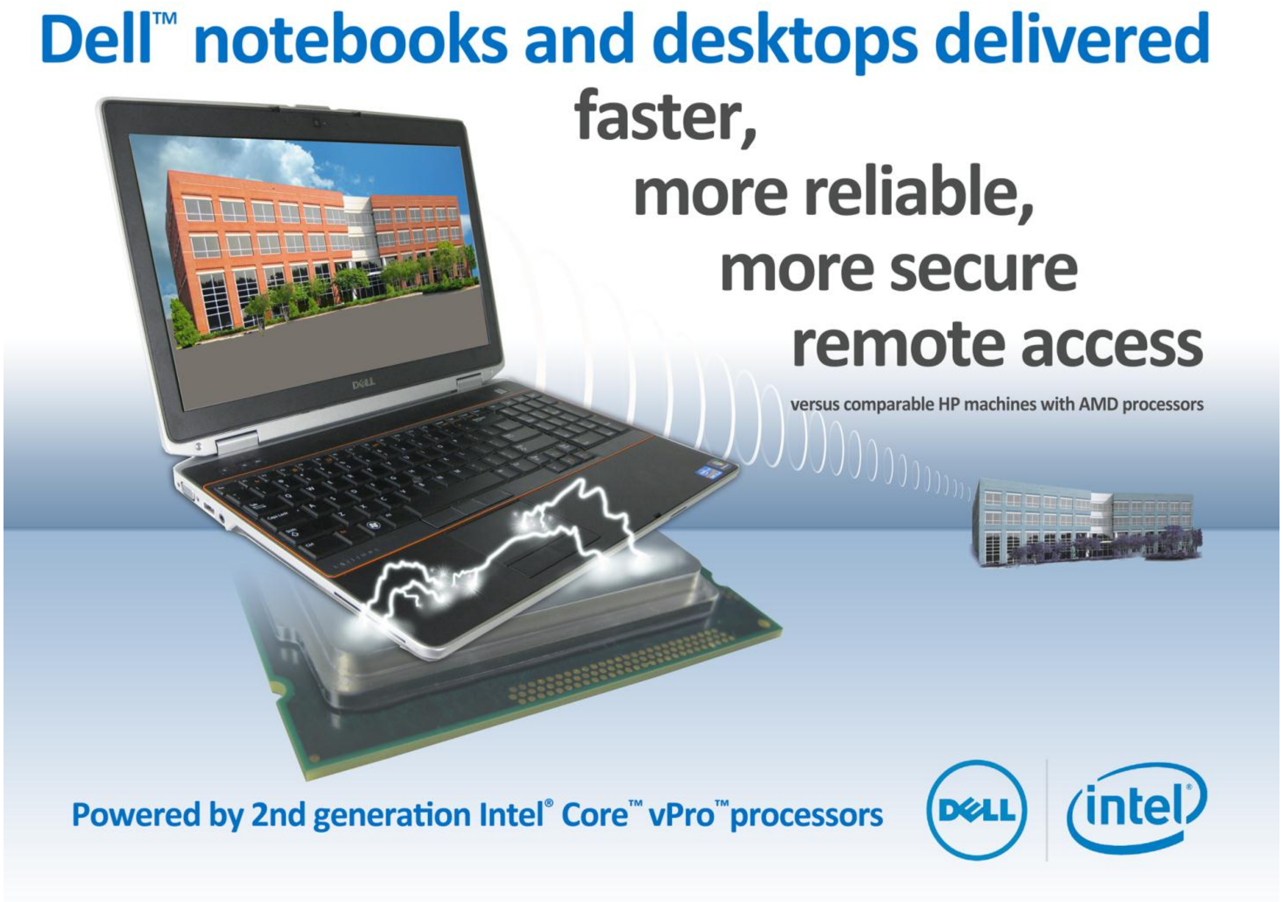
A FEATURE AND PERFORMANCE ANALYSIS OF DELL AND HP NOTEBOOK AND DESKTOP PCS


Dell™ notebooks and desktops delivered
faster,
more reliable,
more secure
remote access
versus comparable HP machines with AMD processors
Powered by 2nd generation Intel® Core™ vPro™ processors
DELL
intel

Your workers and IT staff can be only as productive as their tools let them be. At home and on the road, workers need easy access to confidential documents on the file server. They also need to run their legacy applications on newer operating systems. IT needs to manage workers' systems remotely.

Principled Technologies tested two Windows® features: DirectAccess, for remote file retrieval, and Virtual PC RC (Windows XP Mode), for running legacy Windows XP applications on Windows 7 systems. We compared four 2nd generation Intel Core processor-based Dell systems with Intel vPro technology with four comparable AMD-based HP systems. Using DirectAccess, Dell Latitude™ notebooks retrieved files up to 32.8 percent faster than comparable HP notebooks. The Dell systems also delivered up to 242.1 percent better performance when running applications in Windows XP mode.

We also examined Intel vPro technology's remote management features, which make use of Intel Active Management Technology (AMT). These features make it simple for IT to remotely connect to a user's notebook to offer support.

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

DELL SYSTEMS WITH INTEL VPRO TECHNOLOGY DELIVER

We tested two Dell notebook systems powered by 2nd generation Intel Core vPro processors, a mid-range Dell Latitude E6420 and a high-end Dell Latitude E6520, and two HP notebooks powered by AMD processors, a mid-range HP Pavilion dm1z and a high-end HP Pavilion dv6z Select Edition.

We also tested two Dell desktops powered by 2nd generation Intel Core processors, a mid-range Dell Vostro™ 460 Mini Tower and a high-end Dell OptiPlex™ 990 Mini Tower, and two HP desktops powered by AMD processors, a mid-range HP Pavilion Slimline s5750z and a high-end HP Pavilion p6750z.

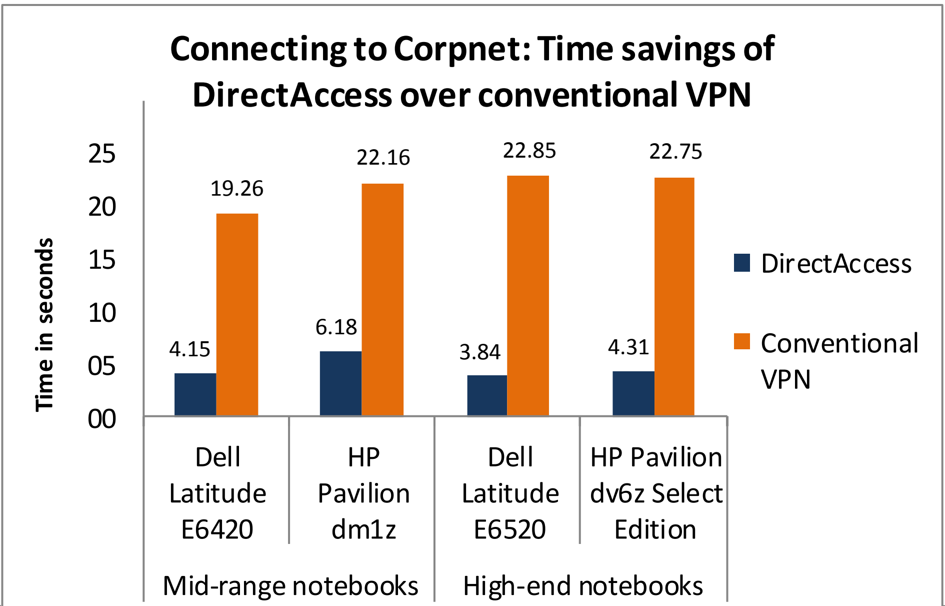
All four Dell systems had Intel vPro technology.

DELL + INTEL MAKE THE MOST OF DIRECTACCESS

DirectAccess is a Windows 7 feature that gives mobile users seamless and secure access to corporate intranet resources when traveling and working from home, without needing to use a VPN. This transparent connection, which is active whenever the user connects to the Internet, can enhance work experience and increase productivity. We configured our notebooks to connect to a DirectAccess server, and tested how long it took to connect to the server using DirectAccess versus manually connecting to the network and accessing shared files over a conventional VPN.

The Intel Core processor-based Dell Latitude notebooks experienced a greater benefit from DirectAccess—as much as 83.2 percent time saved—and connected to the corporate network using DirectAccess faster—as much as 32.8 percent faster—than the corresponding HP Pavilion systems, making Dell a great choice for productivity and user satisfaction for workers when they are offsite.

Figure 1: Time, in seconds, it took the four notebook systems to access a remote file server using DirectAccess and a conventional VPN. Lower numbers are better.



DELL + INTEL LET YOU RUN LEGACY APPLICATIONS WITH STRONG PERFORMANCE

Organizations typically upgrade applications and software at a slower pace than notebook and desktop systems. This means workers find themselves running a new operating system but needing to use an application that runs on only an older OS. A virtual machine running the older OS solves this problem.

Windows XP Mode for Windows 7 allows you to run your Windows XP productivity applications directly from a Windows 7-based PC, and the 2nd generation Intel Core processor boosts the performance you experience when doing so. We ran a performance benchmark, SYSmark Preview 2007 v1.06, on both the native Windows 7 operating system, and in a Windows Virtual PC (Windows XP Mode) to compare the Windows XP virtual machine's performance to the native OS. SYSmark 2007 Preview v1.06 measures system performance in four workload scenarios: e-learning, office productivity, video creation, and 3D modeling. (Learn more about the systems we tested in Appendix A, and more about our testing process in Appendix B.)

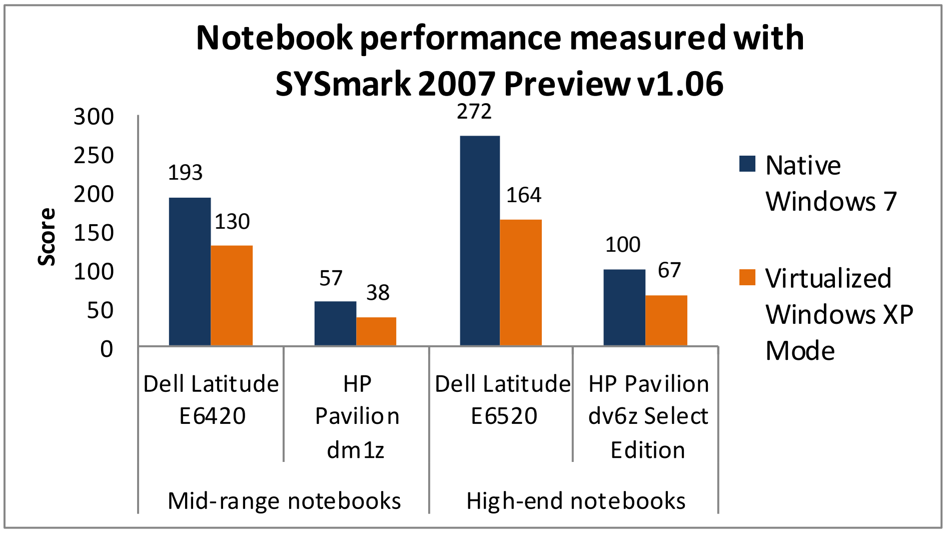


Figure 2: SYSmark 2007 Preview productivity results for the four notebook systems. Higher numbers are better.

Figure 2 shows the BAPCo SYSmark Preview 2007 performance testing results. The Dell Latitude E6420 notebook, with a score of 193, outperformed the HP Pavilion dm1z notebook's score of 57 by 239.0 percent. Even though the Windows XP virtual machine performed lower than the native OS on the Dell Latitude E6420, the virtual machine was still 128.1 percent faster than the HP Pavilion dm1z running its native OS, and 242.1 percent faster than the Windows XP virtual machine on the HP Pavilion dm1z.

The Dell Latitude E6520 notebook, with a score of 272, outperformed the HP Pavilion dv6z Select Edition notebook's score of 100 by 172.0 percent. Even though the Windows XP virtual machine performed lower than the native OS on the Dell Latitude E6520, the virtual machine was still 64.0 percent faster than the HP Pavilion dv6z Select Edition running its native OS, and 145.7 percent faster than the Windows XP virtual machine on the HP Pavilion dv6z Select Edition.

Figure 3: SYSmark 2007 Preview productivity results for the four desktop systems. Higher numbers are better.

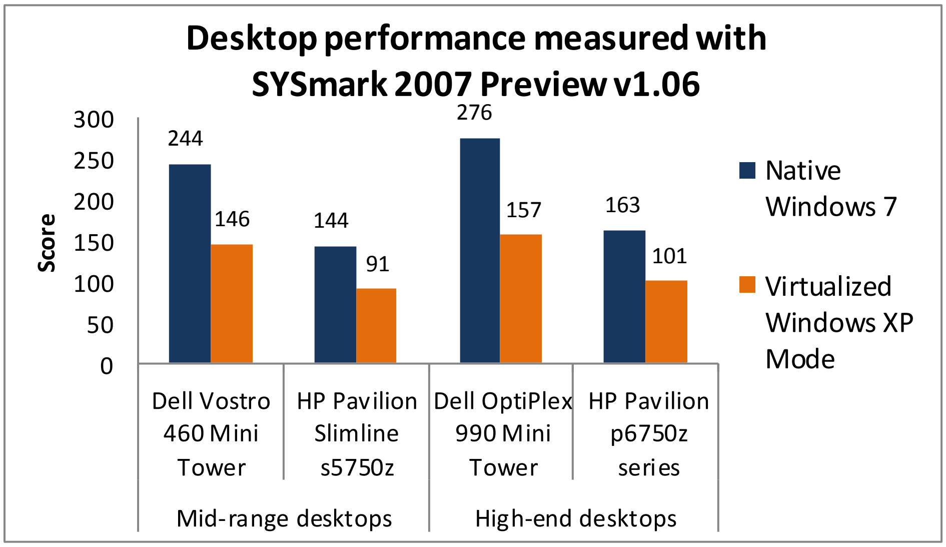


Figure 3 compares the SYSmark 2007 Preview performance results for the four desktop systems running on the native OS and in the Windows XP virtual machine. Both Dell desktops outperformed the HP Pavilion desktops in Windows 7 by about 69 percent. The virtual machines on the Dell desktops performed about equal to the native OS on the HP desktops, and beat the virtual machine performance on the HP desktops by 55 to 60 percent.

INTEL VPRO TECHNOLOGY'S REMOTE MANAGEMENT FEATURES SAVE TIME AND MONEY

Intel Active Management Technology is part of the Intel Management Engine, which is a feature of Intel vPro technology. Intel AMT consists of a set of remote management features that allows remote power up, power down, reboot, access to the BIOS, and access to system information. This feature of 2nd generation Intel Core processors allows a system administrator to monitor and manage vPro-based systems remotely even if the system is not powered on. The AMD-based systems did not ship with this capability.

We set up Intel AMT on the four Dell systems we tested. The fact that this technology is built into the Intel 2nd generation Core processors means that a centralized IT department can ensure a secure system with ease. Using Intel vPro technology, System Center Configuration Manager (SCCM) manages PCs without requiring the IT department to either (1) send an IT administrator to the branch office or (2) incur the cost of shipping systems to the centralized IT department to perform essential security tasks.

TEST RESULTS

Figures 4 and 5 show the time the notebooks took to connect to Corpnet using two methods—DirectAccess and a conventional VPN. These results represent the median of three test runs.

Mid-range notebook systems	Dell Latitude E6420 (Intel Core i5)	HP Pavilion dm1z (AMD Dual-Core)	Percentage improvement with Dell Latitude E6420 (Intel Core i5)
Time to connect to Corpnet using DirectAccess	04.15	06.18	02.03 (32.8%)
Time to connect to Corpnet using a conventional VPN	19.26	22.16	02.90 (13.1%)
Percentage improvement with DirectAccess	15.11 (78.5%)	15.98 (72.1%)	

Figure 4: Connection time, in seconds, for the mid-range notebook systems. Lower numbers are better.

High-end notebook systems	Dell Latitude E6520 (Intel Core i7)	HP Pavilion dV6Z Select Edition (AMD Phenom II)	Percentage improvement with Dell Latitude E6520 (Intel Core i7)
Time to connect to Corpnet using DirectAccess	03.84	04.31	00.47 (10.9%)
Time to connect to Corpnet using a conventional VPN	22.85	22.75	-00.10 (-0.4%)
Percentage improvement with DirectAccess	19.01 (83.2%)	18.44 (81.1%)	

Figure 5: Connection time, in seconds, for the high-end notebook systems. Lower numbers are better.

Figures 6 and 7 show the SYSmark 2007 Preview v1.06 results for the notebook systems, run on the native OS, and in Windows XP mode in a Windows Virtual PC. These results represent the median of three test runs.

Mid-range notebook systems	Dell Latitude E6420 (Intel Core i5)	HP Pavilion dm1z (AMD Dual-Core)	Percentage improvement with Dell Latitude E6420 (Intel Core i5)
BAPCo SYSmark 2007 Preview v1.06 Rating (Windows 7 – native OS)	193	57	239.0%
BAPCo SYSmark 2007 Preview v1.06 Rating (Windows XP mode)	130	38	242.1%

Figure 6: Benchmark score for the mid-range systems. Higher numbers are better.

High-end notebook systems	Dell Latitude E6520 (Intel Core i7)	HP Pavilion dV6Z Select Edition (AMD Phenom II)	Percentage improvement with Dell Latitude E6520 (Intel Core i7)
BAPCo SYSmark 2007 Preview v1.06 Rating (Windows 7 – native OS)	272	100	172.0%
BAPCo SYSmark 2007 Preview v1.06 Rating (Windows XP mode)	164	67	145.7%

Figure 7: Benchmark score for the high-end systems. Higher numbers are better.

Figures 8 and 9 show the SYSmark 2007 Preview v1.06 results for the desktop systems, run on the native OS, and in Windows XP mode in a Windows Virtual PC. These results represent the median of three test runs.

Mid-range desktop systems	Dell Vostro 460 Mini Tower (Intel Core i5)	HP Pavilion Slimline s5750z (AMD Athlon X4)	Percentage improvement with Dell Vostro 460 (Intel Core i5)
BAPCo SYSmark 2007 Preview v1.06 Rating	244	144	69.4%
BAPCo SYSmark 2007 Preview v1.06 Rating (Windows XP mode)	146	91	60.4%

Figure 8: Benchmark score for the mid-range systems. Higher numbers are better.

High-end desktop systems	Dell OptiPlex 990 Mini Tower (Intel Core i7)	HP Pavilion p6750z series (AMD Phenom X4)	Percentage improvement with Dell OptiPlex 990 (Intel Core i7)
BAPCo SYSmark 2007 Preview v1.06 Rating	276	163	69.3%
BAPCo SYSmark 2007 Preview v1.06 Rating (Windows XP mode)	157	101	55.4%

Figure 9: Benchmark score for the high-end systems. Higher numbers are better.

SUMMARY

Workers need easy access to their documents when working remotely and they need to be able to run their legacy applications on newer operating systems with good performance. IT needs to manage workers' systems remotely.

In our tests, we found that Dell Latitude notebooks powered by the Intel Core processor family outperformed comparable HP Pavilion notebooks in connecting to corporate files remotely. We also found that Dell notebooks and desktops powered by the Intel Core processor family outperformed comparable HP systems in running virtual sessions. Finally, the Intel vPro features of the 2nd generation Intel Core processors in the Dell systems provide built-in remote management capabilities that you can't get with an AMD-based system.

With as much as 242.1 percent better performance than HP systems, Dell notebooks and desktops are an excellent choice to meet workers' performance and productivity needs.

APPENDIX A – DETAILED SYSTEM CONFIGURATION INFORMATION

Figure 10 presents each notebook test system and the details of its configuration.

System	Dell Latitude E6420 (Intel Core i5)	Dell Latitude E6520 (Intel Core i7)	HP Pavilion dm1z (AMD Dual-Core)	HP Pavilion dv6z Select Edition (AMD Phenom II)
General				
Number of processor packages	1	1	1	1
Number of cores per processor	2	4	2	4
Number of hardware threads per core	4	8	1	4
System power management policy	Dell	Dell	HP Recommended	HP Recommended
Processor power-saving option	Enhanced Intel SpeedStep® Technology	Enhanced Intel SpeedStep Technology	AMD PowerNow!™ Technology (Cool’n’Quiet™ Technology)	AMD PowerNow! Technology (Cool’n’Quiet Technology)
System dimensions (length x width x height)	13-7/8” x 9-4/8” x 1-3/8”	15-1/8” x 10-1/4" x 1-3/8”	11-4/8” x 8-3/8” x 1-1/8”	15” x 9-7/8” x 1-3/8”
System weight	5 lbs. 5 oz.	6 lbs. 5 oz.	3 lbs. 6 oz.	5 lbs. 8 oz.
CPU				
Vendor	Intel	Intel	AMD	AMD
Name	Core i5	Core i7	Dual-Core Processor	Phenom II
Model number	2520M	2720QM	E-350	N970
Stepping	D2	D2	B0	BL-C3
Socket type and number of pins	Socket 988B rPGA	Socket 988B rPGA	Socket FT1 BGA	Socket S1 (638)
Core frequency (GHz)	2.50	2.20	1.60	2.20
L1 cache	32 KB + 32 KB (per core)	32 KB + 32 KB (per core)	32 KB + 32 KB (per core)	64 KB + 64 KB (per core)
L2 cache	512 KB (256 KB per core)	1 MB (256 KB per core)	1 MB (512 KB per core)	2 MB (512 KB per core)
L3 cache	3 MB	6 MB	N/A	N/A
Platform				
Vendor	Dell	Dell	HP	HP
Motherboard model number	0K0DNP	OJ4TFW	1611	1640

System	Dell Latitude E6420 (Intel Core i5)	Dell Latitude E6520 (Intel Core i7)	HP Pavilion dm1z (AMD Dual-Core)	HP Pavilion dv6z Select Edition (AMD Phenom II)
Motherboard chipset	Intel QM67	Intel QM67	AMD A40/A50 Series FCH	AMD 785GX
BIOS name and version	Dell A01 (03/02/2011)	Dell A01 (03/02/2011)	HP F.05 (03/04/2011)	HP F.25 (02/15/2011)
Memory module(s)				
Vendor and model number	Micron® 8JSF25664HZ-1G4D1	Samsung M471B5273DHO-CH9	Hyundai HMT325S6BFR8C-H9	Micron 16JSF51264HZ-1G4D1
Type	PC3-10600S	PC3-10600S	PC3-10600	PC3-10600S
Speed (MHz)	1,333	1,333	1,333	1,333
Speed running in the system (MHz)	1,333	1,333	1,066	1,333
Timing/Latency (tCL-tRCD-tRP-tRASmin)	9-9-9-24	9-9-9-24	7-7-7-20	9-9-9-24
Size (MB)	4,096	8,192	4,096	8,192
Number of memory module(s)	2 x 2,048 MB	2 x 4,096 MB	2 x 2,048 MB	2 x 4,096 MB
Chip organization (single-sided/double-sided)	Double-sided	Double-sided	Double-sided	Double-sided
Channel (single/dual)	Dual	Dual	Dual	Dual
Hard disk				
Vendor and model number	Western Digital WD2500BEKT-75PVMT0	Samsung SSD PM810	Seagate ST9250410AS	Samsung HM640JJ
Number of disks in system	1	1	1	1
Size (GB)	250	128	250	640
Buffer size (MB)	16	128	16	16
RPM	7,200	N/A	7,200	7,200
Type	SATA 3.0 Gb/s	SATA II 3.0 Gb/s	SATA 3.0 Gb/s	SATA 3.0 Gb/s
Controller	Intel QM67	Intel QM67	AMD A40/A50 Series FCH	AMD SB800
Driver	Intel 10.1.0.1008 (11/06/2010)	Intel 10.1.0.1008 (11/06/2010)	Microsoft 6.1.7600.20713 (06/21/2006)	Microsoft 6.1.7600.20713 (06/21/2006)

System	Dell Latitude E6420 (Intel Core i5)	Dell Latitude E6520 (Intel Core i7)	HP Pavilion dm1z (AMD Dual-Core)	HP Pavilion dv6z Select Edition (AMD Phenom II)
Operating system				
Name	Windows 7 Ultimate	Windows 7 Professional	Windows 7 Professional	Windows 7 Professional
Build number	7600	7600	7600	7600
Service Pack	N/A	N/A	N/A	N/A
File system	NTFS	NTFS	NTFS	NTFS
Kernel	ACPI x64-based PC	ACPI x64-based PC	ACPI x64-based PC	ACPI x64-based PC
Language	English	English	English	English
Microsoft DirectX® version	DirectX 11	DirectX 11	DirectX 11	DirectX 11
Graphics 1				
Vendor and model number	Intel HD Graphics 3000	NVIDIA® NVS 4200M	AMD Radeon™ HD 6310M	ATI Mobility Radeon HD 6550
Type	Integrated	Discrete	Integrated	Discrete
Chipset	Intel HD Graphics Family	NVS 4200M	ATI Radeon HD 6310M	ATI Mobility Radeon HD 6550
BIOS version	2089.11	75.19.17.1.2	BR39197.bin	BR38060.010
Total available graphics memory (MB)	1,696	4,095	1,972	4,083
Dedicated video memory (MB)	64	512	384	1,024
System video memory (MB)	0	0	0	0
Shared system memory (MB)	1,632	3,583	1,588	3,059
Resolution	1,366 x 768 x 32-bit	1,920 x 1,080 x 32-bit	1,366 x 768 x 32-bit	1,366 x 768 x 32-bit
Driver	Intel 8.15.10.2266 (12/16/2010)	NVIDIA 8.17.12.6696 (02/02/2011)	ATI Technologies Inc. 8.792.0.0 (11/09/2010)	ATI Technologies Inc. 8.770.2.2000 (09/29/2010)
Graphics 2				
Vendor and model number	N/A	N/A	N/A	AMD M880G with ATI Mobility Radeon HD 4250
Type	N/A	N/A	N/A	Integrated
Chipset	N/A	N/A	N/A	ATI Mobility Radeon HD 4250

System	Dell Latitude E6420 (Intel Core i5)	Dell Latitude E6520 (Intel Core i7)	HP Pavilion dm1z (AMD Dual-Core)	HP Pavilion dv6z Select Edition (AMD Phenom II)
BIOS version	N/A	N/A	N/A	VER010.094.001.045.035812
Total available graphics memory (MB)	N/A	N/A	N/A	3,131
Dedicated video memory (MB)	N/A	N/A	N/A	320
System video memory (MB)	N/A	N/A	N/A	0
Shared system memory (MB)	N/A	N/A	N/A	2,811
Resolution	N/A	N/A	N/A	1,366 x 768 x 32-bit
Driver	N/A	N/A	N/A	ATI Technologies Inc. 8.770.2.2000 (09/29/2010)
Sound card/subsystem				
Vendor and model number	Intel Display Audio	NVIDA High Definition Audio	ATI High Definition Audio Device	ATI High Definition Audio Device
Driver	Intel 6.14.0.3074 (10/15/2010)	NVIDIA 1.2.14.0 (12/13/2010)	ATI Technologies Inc. 7.11.0.7710 (08/30/2010)	ATI Technologies Inc. 7.11.0.7706 (05/06/2010)
Ethernet				
Vendor and model number	Intel 82579LM Gigabit	Intel 82579LM Gigabit	Realtek PCIe GBE Family	Realtek PCIe GBE Family
Driver	Intel 11.8.81.0 (10/28/2010)	Intel 11.8.81.0 (10/28/2010)	Realtek 7.27.920.2010 (09/20/2010)	Realtek 7.23.623.2010 (06/23/2010)
Wireless				
Vendor and model number	Intel Centrino™ Ultimate-N 6300 AGN	Intel Centrino Ultimate-N 6300 AGN	Ralink RT5390	Broadcom® 43224AG
Driver	Intel 14.0.1.2 (12/21/2010)	Intel 14.0.1.2 (12/21/2010)	Ralink Technology Corp. 3.1.13.0 (11/04/2010)	Broadcom 5.60.350.11 (05/07/2010)
Optical drive(s)				
Vendor and model number	TSSTcorp TS-U333B	TSSTcorp TS-U633J	HP HSTNN-ID06	HP TS-L633R
Type	DVD ROM	DVD+/-RW	BD-ROM	CD/DVD-RW

System	Dell Latitude E6420 (Intel Core i5)	Dell Latitude E6520 (Intel Core i7)	HP Pavilion dm1z (AMD Dual-Core)	HP Pavilion dv6z Select Edition (AMD Phenom II)
USB ports				
Number	3	3	3	3
Type	2.0	2.0	2.0	2.0
Other	eSATA, Media Card Reader	eSATA, HDMI, Media Card Reader	HDMI, Media Card Reader	eSATA, HDMI, Media Card Reader
Monitor				
LCD type	HD LED WXGA	HD LED WXGA	HD LED WXGA	HD LED WXGA
Screen size	14”	15.6”	11.6”	15.6”
Refresh rate(Hz)	60	60	60	60
Battery				
Type	T54FJ Lithium-ion	T54FJ Lithium-ion	HSTNN-OB2D Lithium-ion	HSTNN-DBOX Lithium-ion
Size (length x width x height)	8-1/8” x 2” x 3/4"	8-1/8” x 2” x 3/4"	8” x 2-3/8” x 1”	8” x 2” x 7/8”
Rated capacity	5400mAh/ 11.1V (60Wh)	5400mAh/ 11.1V (60Wh)	5100 mAh / 10.8V (55Wh)	5100 mAh / 10.8V (55Wh)
Weight	11 oz.	11 oz.	11 oz.	11 oz.

Figure 10: Configuration information for the four notebook test systems.

Figure 11 presents each desktop test system and the details of its configuration.

System	Dell Vostro 460 Mini Tower (Intel Core i5-2400)	Dell OptiPlex 990 Mini Tower (Intel Core i7-2600)	HP Pavilion Slimline s5750z (AMD Athlon II X4 640)	HP Pavilion p6750z (AMD Phenom II X4 840)
General				
Number of processor packages	1	1	1	1
Number of cores per processor	4	4	4	4
Number of hardware threads per core	4	8	4	4
System power management policy	Dell	Dell	Balanced	Balanced
Processor power-saving option	Enhanced Intel SpeedStep® Technology	Enhanced Intel SpeedStep Technology	AMD PowerNow!™ Technology (Cool'n'Quiet™ Technology)	AMD PowerNow! Technology (Cool'n'Quiet Technology)
System dimensions (length x width x height)	17.5" x 7" x 14.25"	16.5" x 7" x 14.25"	15.25" x 4.5" x 12.25"	16.5" x 7" x 15.75"
System weight (lbs.)	22	20	13	18
CPU				
Vendor	Intel	Intel	AMD	AMD
Name	Core i5	Core i7	Athlon II X4	Phenom II X4
Model number	2400	2600	640	840
Stepping	D2	D2	PH-E0	PH-E0
Socket type and number of pins	Socket 1155 LGA	Socket 1155 LGA	Socket AM3 (938)	Socket AM3 (938)
Core frequency (GHz)	3.10	3.40	3.00	2.90
Bus frequency	5 GT/s	5 GT/s	4,000 MHz HyperTransport™ Technology	2,000 MHz HyperTransport Technology
L1 cache	32 KB + 32 KB (per core)	32 KB + 32 KB (per core)	64 KB + 64 KB (per core)	64 KB +64 KB (per core)
L2 cache	1 MB (256 KB per core)	1 MB (256 KB per core)	2 MB (512 KB per core)	2 MB (512 KB per core)
L3 cache	6 MB	8 MB	N/A	6 MB
Platform				
Vendor	Dell	Dell	FOXCONN	FOXCONN
Motherboard model number	OY2MRG	06D7TR	2B1	2AB1

System	Dell Vostro 460 Mini Tower (Intel Core i5-2400)	Dell OptiPlex 990 Mini Tower (Intel Core i7-2600)	HP Pavilion Slimline s5750z (AMD Athlon II X4 640)	HP Pavilion p6750z (AMD Phenom II X4 840)
Motherboard chipset	H67	ID1C4E	AMD 785G	AMD 785G
BIOS name and version	Dell A03 (02/15/2011)	Dell Inc. A02 (02/26/2011)	American Megatrends Inc. 6.06 (03/22/2011)	American Megatrends Inc. 6.06 (03/22/2011)
Memory module(s)				
Vendor and model number	Micron Tech. 8JTF25664AZ-1G4D1	Samsung M378B5273DH0-CH9	Samsung M378B5773CH0-CH9	Hyundai HMT125U6TFR8C-H9
Type	PC3-10600	PC3-10600	PC3-10600	PC3-10600
Speed (MHz)	1,333	1,333	1,333	1,333
Speed running in the system (MHz)	1,333	1,333	1,333	1,333
Timing/Latency (tCL-tRCD-tRP-tRASmin)	9-9-9-24	9-9-9-24	9-9-9-24	9-9-9-24
Size (MB)	4,096	8,192	4,096	8,192
Number of memory module(s)	2 x 2,048 MB	2 x 4,096 MB	2 x 2,048 MB	4 x 2,048 MB
Chip organization (single-sided/double-sided)	Single-sided	Double-sided	Single-sided	Double-sided
Channel (single/dual)	Dual	Dual	Dual	Dual
Hard disk				
Vendor and model number	Western Digital WD5000AAKX-753CA0	Seagate ST3500413AS	Western Digital WD50000AAKS-60Z1A0	Seagate ST31500341AS
Number of disks in system	1	1	1	1
Size (GB)	500	500	500	1,500
Buffer size (MB)	16	16	16	32
RPM	7,200	7,200	7,200	7,200
Type	SATA 3Gb/s	SATA 3Gb/s	SATA 3Gb/s	SATA 3Gb/s
Controller	Intel H67	Intel ID1C4E	AMD SB700	AMD SB700
Driver	Intel 10.0.0.1046 (09/13/2010)	Intel 10.1.0.1008 (11/06/2010)	AMD 1.2.1.238 (10/08/2010)	AMD 1.2.1.238 (10/08/2010)
Operating system				
Name	Windows® 7 Ultimate	Windows 7 Ultimate	Windows 7 Ultimate	Windows 7 Ultimate
Build number	7600	7600	7600	7600

System	Dell Vostro 460 Mini Tower (Intel Core i5-2400)	Dell OptiPlex 990 Mini Tower (Intel Core i7-2600)	HP Pavilion Slimline s5750z (AMD Athlon II X4 640)	HP Pavilion p6750z (AMD Phenom II X4 840)
Service Pack	SP1 (for SPEC CPU2006 testing only)	SP1 (for SPEC CPU2006 testing only)	SP1 (for SPEC CPU2006 testing only)	SP1 (for SPEC CPU2006 testing only)
File system	NTFS	NTFS	NTFS	NTFS
Kernel	ACPI x64 – based PC	ACPI x64 – based PC	ACPI x64 – based PC	ACPI x64 – based PC
Language	English	English	English	English
Microsoft DirectX® version	DirectX 11	DirectX 11	DirectX 11	DirectX 11
Graphics				
Vendor and model number	AMD Radeon™ HD 6450	2 x AMD Radeon HD 6450	AMD Radeon HD 4200	AMD Radeon HD 6570
Type	Discrete	Discrete	Discrete	Discrete
Chipset	ATI Radeon HD 6450	ATI Radeon HD 6450	ATI Radeon HD 4200	ATI Radeon HD 6570
BIOS version	113-AD00200-101-PE	113-C2640500-100	BR34448.bin	113-AC89900-102-PE
Total available graphics memory (MB)	2,807	4,851	1,919	4,083
Dedicated video memory (MB)	1,024	2,048	256	1,024
System video memory (MB)	0	0	0	0
Shared system memory (MB)	1,783	2,803	1,663	3,059
Resolution	1,280 x 1,024 x 32-bit	1,280 x 1,024 x 32-bit	1,280 x 1,024 x 32-bit	1,280 x 1,024 x 32-bit
Driver	ATI Technologies Inc. 8.812.0.0 (01/04/2011)	ATI Technologies Inc. 8.783.2.2000 (11/16/2010)	ATI Technologies Inc. 8.733.0.0 (05/11/2010)	ATI Technologies Inc. 8.784.1.0 (11/23/2010)
Sound card/subsystem				
Vendor and model number	Realtek High Definition Audio	Realtek High Definition Audio	Realtek High Definition Audio	Creative SB X-Fi
Driver	Realtek Semiconductor Corp. 6.0.1.6141 (06/22/2010)	Realtek Semiconductor Corp. 6.0.1.5883 (09/14/2010)	Realtek Semiconductor Corp. 6.0.1.6196 (09/07/2010)	Creative 6.0.1.6 (03/05/2010)

System	Dell Vostro 460 Mini Tower (Intel Core i5-2400)	Dell OptiPlex 990 Mini Tower (Intel Core i7-2600)	HP Pavilion Slimline s5750z (AMD Athlon II X4 640)	HP Pavilion p6750z (AMD Phenom II X4 840)
Ethernet				
Vendor and model number	Broadcom NetLink Gigabit	Intel 82579LM Gigabit	Realtek PCIe FE Family	Realtek PCIe FE Family
Driver	Broadcom 14.2.0.7 (07/20/2010)	Intel 11.8.81.0 (10/28/2010)	Realtek 7.26.902.2010 (09/02/2010)	Realtek 7.26.902.2010 (09/02/2010)
Optical drive(s)				
Vendor and model number	HL-DT-ST CH20N	TSSTcorp TS-H653H	HP DH16ABLH	HP DH16ABLH
Type	BD-ROM	CD/DVD-RW	CD/DVD-RW	CD/DVD-RW
USB ports				
Number	8	10	6	6
Type	2.0	2.0	2.0	2.0
Other	eSATA, HDMI, Media Card Reader	eSATA	Media Card Reader	Media Card Reader
Monitor				
LCD type	Optiquest® Q7	Optiquest Q7	Optiquest Q7	Optiquest Q7
Screen size	17”	17”	17”	17”
Refresh rate (Hz)	60	60	60	60

Figure 11: Configuration information for the four desktop test systems.

APPENDIX B – ABOUT OUR TESTING

Detailed test methodology

Measuring performance with BAPCo SYSmark 2007 Preview v1.06

Setting up the test

Prior to installing SYSmark 2007 Preview, we installed both Virtual PC RC and Virtual XP Mode. We installed all applicable Windows updates in Virtual XP Mode. We allocated 4GB of memory to Virtual XP Mode before installing and running SYSmark 2007 Preview v1.06.

1. Disable the User Account Control.
    a. Click Start→Control Panel.
    b. At the User Accounts and Family Safety settings screen, click Add or remove user account.
    c. At the User Account Control screen, click Continue.
    d. Click Go to the main User Accounts page.
    e. At the Make changes to your user account screen, click Turn User Account Control on or off.
    f. At the User Account Control screen, click Continue.
    g. Uncheck Use User Account Control to help protect your computer, and click OK.
    h. At the You must restart your computer to apply these changes screen, click Restart Now.
2. Purchase and install SYSmark 2007 Preview v1.06 from https://www.bapcostore.com/store/product.php?productid=16165&cat=251&page=1.
3. At the Welcome to InstallShield Wizard screen, click Next.
4. At the License Agreement screen, select I accept the terms in the License Agreement, and click Next.
5. At the Choose Destination Location screen, click Next.
6. At the Ready to Install the Program screen, click Install.
7. When the installation is complete, click Finish.

CONFIGURING THE NETWORK INFRASTRUCTURE FOR DIRECTACCESS TESTING

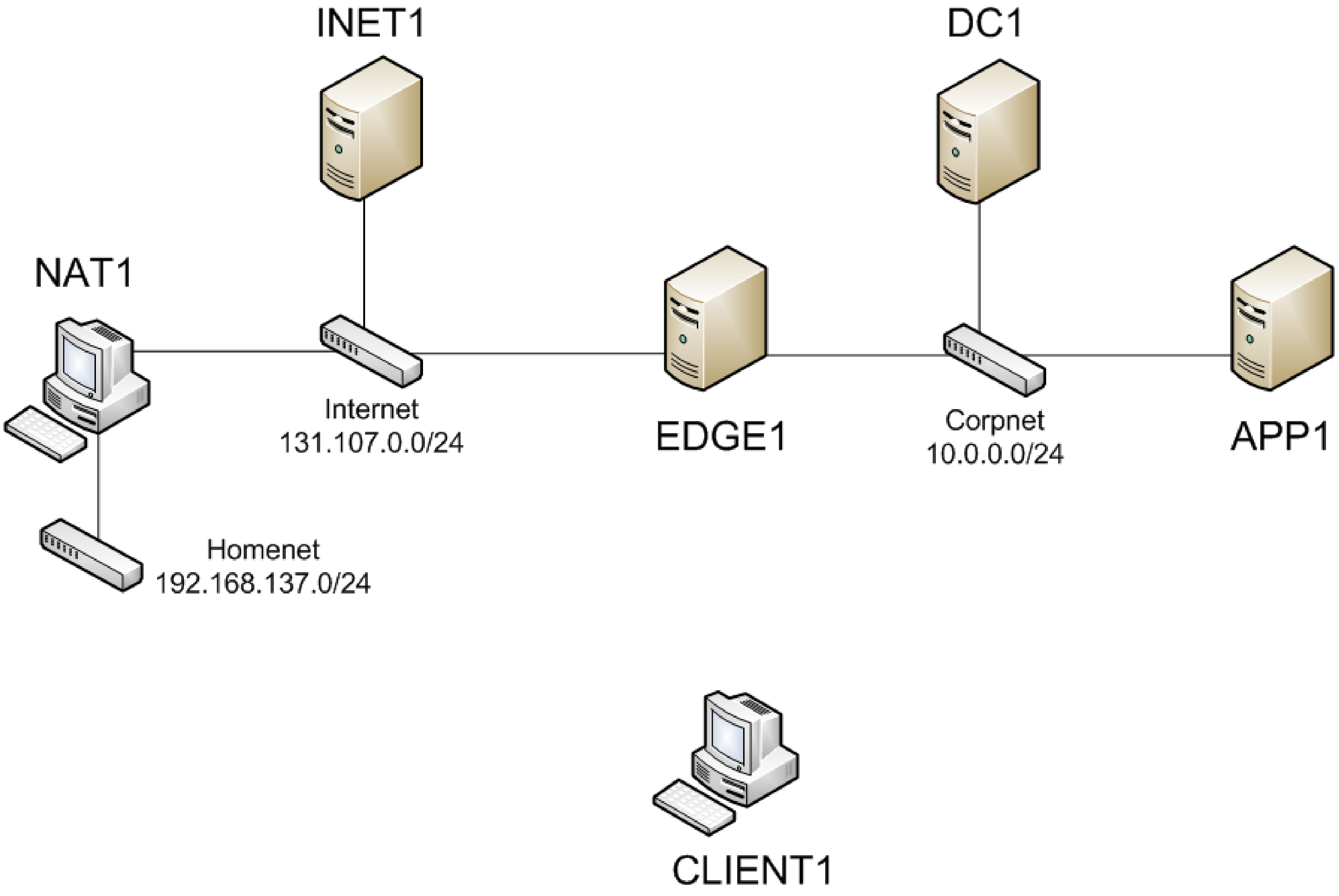


Figure 12: Testing configuration.

Setting up and configuring the domain controller (DC1)

Installing Windows Server 2008 R2 SP1 on DC1

1. Insert the installation DVD for Windows Server 2008 SP2 x64 into the DVD drive.
2. Choose the language, time and currency, and keyboard input. Click Next.
3. Click Install Now.
4. Choose Windows Server Enterprise (Full Installation). Click Next.
5. Accept the license terms, and click Next.
6. Click Custom.
7. Click the Disk, and click Drive options (advanced).
8. Click New, Apply, Format, and click Next.
9. Let the installation process continue. The server will reboot several times.
10. After the installation completes, click OK to set the Administrator password.
11. Enter the administrator password twice, and click OK.
12. Click Start→Control Panel, and double-click System.

13. Click Change Settings.
14. Click Change.
15. Enter the new computer name, and click OK.
16. Click OK to restart, click Close, and click Restart Now.

Installing Windows updates on DC1

We used the Windows Update feature to install the following updates:

- Windows Internet Explorer 9
- Security Update for Microsoft Windows (KB2524375)
- Security Update for Microsoft Windows (KB2511455)
- Security Update for Microsoft Windows (KB2510531)
- Security Update for Microsoft Windows (KB2509553)
- Security Update for Microsoft Windows (KB2508429)
- Security Update for Microsoft Windows (KB2508272)
- Security Update for Microsoft Windows (KB2507618)
- Security Update for Microsoft Windows (KB2506223)
- Security Update for Microsoft Windows (KB2506212)
- Security Update for Microsoft Windows (KB2506014)
- Security Update for Microsoft Windows (KB2503658)
- Security Update for Microsoft Windows (KB2497640)
- Security Update for Microsoft Windows (KB2425227)
- Security Update for Microsoft Windows (KB2446710)
- Security Update for Microsoft Windows (KB976902)

Configuring TCP/IP on DC1

1. In Initial Configuration Tasks, click Configure networking.
2. In Network Connections, right-click Local Area Connection, and click Properties.
3. Click Internet Protocol Version 4 (TCP/IPv4), and click Properties.
4. Select Use the following IP address. IP address, type `10.0.0.1`. In Subnet mask, type `255.255.255.0`. Select Use the following DNS server addresses. In Preferred DNS server, type `10.0.0.1`.
5. Click Advanced, and click the DNS tab.
6. In DNS suffix for this connection, type `corp.satie.com`, click OK twice, and click Close.
7. Close the Network Connections window.
8. In Initial Configuration Tasks, click Provide computer name and domain.
9. In System Properties, click Change. In Computer name, type `DC1`, click OK twice, and click Close. When you are prompted to restart the computer, click Restart Now.
10. After restarting, log in using the local administrator account.
11. In Initial Configuration Tasks, click Do not show this window at logon, and click Close.

Configuring DC1 as a domain controller and DNS server

1. In the console tree of Server Manager, click Roles. In the details pane, click Add Roles, and click Next.
2. On the Select Server Roles page, click Active Directory® Domain Services, click Add Required Features, click Next twice, and click Install. When installation is complete, click Close.

3. To start the Active Directory Installation Wizard, click Start, type `dcpromo`, and press Enter.
4. In the Active Directory Installation Wizard dialog box, click Next twice.
5. On the Choose a Deployment Configuration page, click Create a new domain in a new forest, and click Next.
6. On the Name the Forest Root Domain page, type `corp.satie.com`, and click Next.
7. On the Set Forest Functional Level page, in Forest Functional Level, click Windows Server 2008 R2, and click Next.
8. On the Additional Domain Controller Options page, click Next, click Yes to continue, and click Next.
9. On the Directory Services Restore Mode Administrator Password page, type a strong password twice, and click Next.
10. On the Summary page, click Next.
11. Wait while the wizard completes the configuration of Active Directory and DNS services, and click Finish.
12. When the wizard prompts you to restart the computer, click Restart Now.
13. After the computer restarts, log into the CORP domain using the Administrator account.

Installing and configuring the DHCP server role

1. In the console tree of Server Manager, click Roles.
2. In the details pane, under Roles Summary, click Add roles, and click Next.
3. On the Select Server Roles page, click DHCP Server, and click Next twice.
4. On the Select Network Connection Bindings page, verify that 10.0.0.1 is selected, and click Next.
5. On the Specify IPv4 DNS Server Settings page, verify that corp.satie.com is listed under Parent domain.
6. Type `10.0.0.1` under Preferred DNS server IP address, and click Validate. Verify that the result returned is Valid, and click Next.
7. On the Specify WINS Server Settings page, accept the default setting of WINS is not required on this network, and then click Next.
8. On the Add or Edit DHCP Scopes page, click Add.
9. In the Add Scope dialog box, next to Scope Name, type `Corpnet`. Next to Starting IP Address, type `10.0.0.100`, next to Ending IP Address, type `10.0.0.150`, and next to Subnet Mask, type `255.255.255.0`. Click OK, and click Next.
10. On the Configure DHCPv6 Stateless Mode page, select Disable DHCPv6 stateless mode for this server, and click Next.
11. On the Authorize DHCP Server page, select Use current credentials. Verify that CORP\Administrator is displayed next to User Name, and click Next.
12. On the Confirm Installation Selections page, click Install.
13. Verify the installation was successful, and click Close.

Installing an enterprise root CA on DC1

1. In the console tree of Server Manager, click Roles.
2. Under Roles Summary, click Add roles, and click Next.
3. On the Select Server Roles page, click Active Directory Certificate Services, and click Next twice.
4. On the Role Services page, click Next.
5. On the Setup Type page, click Enterprise, and click Next.
6. On the CA Type page, click Root CA, and click Next.
7. On the Private Key page, click Create a new private key, and click Next.

8. On the Cryptography page, click Next.
9. On the CA Name page, click Next.
10. On the Validity Period page, click Next.
11. On the Certificate Database page, click Next.
12. On the Confirm Installation Selections page, click Install.
13. On the Results page, click Close.

Configuring the CRL distribution settings on DC1

1. On DC1, click Start→Administrative Tools, and click Certification Authority.
2. In the details pane, right-click corp-DC1-CA, and click Properties.
3. In the corp-DC1-CA Properties dialog box, click the Extensions tab.
4. On the Extensions tab, click Add. In Location, type `http://crl.corp.satie.com/crld/`
5. In Variable, click <CAName>, and click Insert.
6. In Variable, click <CRLNameSuffix>, and click Insert.
7. In Variable, click <DeltaCRLAllowed>, and click Insert.
8. In Location, type `.crl` at the end of the Location string, and click OK.
9. Select Include in CRLsand Include in the CDP extension of issued certificates, and click Apply. In the dialog box asking you to restart Active Directory Certificate Services, click No.
10. Click Add.
11. In Location, type `\\app1\crldist$\`
12. In Variable, click <CAName>, and click Insert.
13. In Variable, click <CRLNameSuffix>, and click Insert.
14. In Variable, click <DeltaCRLAllowed>, and click Insert.
15. In Location, type `.crl` at the end of the string, and click OK.
16. Select Publish CRLs to this location and Publish Delta CRLs to this location, and click OK.
17. Click Yes to restart Active Directory Certificate Services.
18. Close the Certification Authority console.

Creating a DNS record for crl.corp.satie.com on DC1

1. On DC1, click Start→Administrative Tools, and click DNS.
2. In the DNS Manager console, expand DC1 and then expand Forward Lookup Zones. Right-click corp.satie.com, and click New Host (A or AAAA).
3. In the New Host dialog box, type `CRL` in Name (uses parent domain name if blank). In IP address, type `10.0.0.3`. Click Add Host.
4. In the DNS dialog box informing you that the record was created, click OK.
5. In the New Host dialog box, click Done.
6. Close the DNS Manager console.

Creating a user account in Active Directory

1. Click Start→Administrative Tools, and click Active Directory Users and Computers.
2. In the console tree, open corp.satie.com, right-click Users→New, and click User.
3. In the New Object - User dialog box, in Full name, type `User1`, and in User logon name, type `User1`.
4. Click Next.
5. In Password, type the password that you want to use for this account, and in Confirm password, type the password again.

6. Clear User must change password at next logon and select Password never expires.
7. Click Next, and click Finish.
8. In the console tree, click Users.
9. In the details pane, double-click Domain Admins.
10. In the Domain Admins Properties dialog box, click the Members tab, and click Add.
11. Under Enter the object names to select (examples), type User1, and click OK twice.
12. Close the Active Directory Users and Computers console.

Configuring computer certificate auto-enrollment in Group Policy

1. Click Start, click Administrative Tools, and click Group Policy Management.
2. In the console tree, open Forest: corp.satie.com\Domains\corp.satie.com.
3. In the details pane, right-click Default Domain Policy, and click Edit.
4. In the console tree of the Group Policy Management Editor, open Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies.
5. In the details pane, right-click Automatic Certificate Request Settings→New, and click Automatic Certificate Request.
6. In the Automatic Certificate Request Wizard, click Next.
7. On the Certificate Template page, click Computer, click Next, and click Finish.
8. Leave the Group Policy Management Editor and Group Policy Management consoles open for the next procedure.

Configuring the maximum computer account password age in Group Policy

1. In the console tree of the Group Policy Management Editor, open Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options.
2. In the details pane, double-click Domain member: Maximum machine account password age.
3. On the Security Policy Setting tab, select Define this policy setting, type 999, and click OK.
4. Close the Group Policy Management Editor and Group Policy Management consoles.

Setting up the Web server and file server (APP1)

Installing Windows Server 2008 R2 SP1 on APP1

1. Insert the installation DVD for Windows Server 2008 SP2 x64 into the DVD drive.
2. Choose the language, time and currency, and keyboard input. Click Next.
3. Click Install Now.
4. Choose Windows Server Enterprise (Full Installation). Click Next.
5. Accept the license terms, and click Next.
6. Click Custom.
7. Click the Disk, and click Drive options (advanced).
8. Click New, Apply, Format, and click Next.
9. Let the installation process continue. The server will reboot several times.
10. After the installation completes, click OK to set the Administrator password.
11. Enter the administrator password twice, and click OK.
12. Click Start→Control Panel, and double-click System.
13. Click Change Settings.
14. Click Change.
15. Enter the new computer name, and click OK.

16. Click OK to restart, click Close, and click Restart Now.

Installing Windows updates on APP1

We used the Windows Update feature to install the following updates:

- Windows Internet Explorer 9
- Security Update for Microsoft Windows (KB2524375)
- Security Update for Microsoft Windows (KB2511455)
- Security Update for Microsoft Windows (KB2510531)
- Security Update for Microsoft Windows (KB2509553)
- Security Update for Microsoft Windows (KB2508429)
- Security Update for Microsoft Windows (KB2508272)
- Security Update for Microsoft Windows (KB2507618)
- Security Update for Microsoft Windows (KB2506223)
- Security Update for Microsoft Windows (KB2506212)
- Security Update for Microsoft Windows (KB2506014)
- Security Update for Microsoft Windows (KB2503658)
- Security Update for Microsoft Windows (KB2497640)
- Security Update for Microsoft Windows (KB2425227)
- Security Update for Microsoft Windows (KB2446710)
- Security Update for Microsoft Windows (KB976902)

Configuring TCP/IP properties

1. In Initial Configuration Tasks, click Configure networking.
2. In the Network Connections window, right-click Local Area Connection, and click Properties.
3. Click Internet Protocol Version 4 (TCP/IPv4), and click Properties.
4. Select Use the following IP address. In IP address, type `10.0.0.3`. In Subnet mask, type `255.255.255.0`.
5. Select Use the following DNS server addresses. In Preferred DNS server, type `10.0.0.1`.
6. Click Advanced, and click the DNS tab. In DNS suffix for this connection, type `corp.satie.com`, click OK twice, and click Close.
7. Close the Network Connections window and leave the Initial Configuration Tasks window open.
8. To check name resolution and network communication between APP1 and DC1, click Start, click All Programs, click Accessories, and click Command Prompt.
9. In the Command Prompt window, type `ping dc1.corp.satie.com`.
10. Verify that there are four replies from 10.0.0.1.
11. Close the Command Prompt window.

Joining APP1 to the CORP domain

1. In Initial Configuration Tasks, click Provide Computer Name and Domain.
2. In the System Properties dialog box, on the Computer Name tab, click Change.
3. In Computer Name, type APP1. In Member of, click Domain, and type `corp.satie.com`.
4. Click OK.
5. When you are prompted for a user name and password, type User1 and its password, and then click OK.
6. When you see a dialog box welcoming you to the corp.satie.com domain, click OK.

7. When you are prompted that you must restart the computer, click OK.
8. On the System Properties dialog box, click Close.
9. When you are prompted to restart the computer, click Restart Now.
10. After the computer restarts, click Switch User, click Other User, and log onto the CORP domain with the User1 account.
11. In Initial Configuration Tasks, click Do not show this window at logon, and click Close.

Installing the Web Server (IIS) role

1. In the console tree of Server Manager, click Roles. In the details pane, click Add Roles, and click Next.
2. On the Select Server Roles page, select Web Server (IIS), and click Next three times.
3. Click Install.
4. Verify that the installation was successful, and click Close.

Creating a Web-based CRL distribution point

1. Click Start→Administrative Tools, and click Internet Information Services (IIS) Manager.
2. In the console tree, navigate to APP1\Sites\Default Web Site. Right-click Default Web Site and click Add Virtual Directory.
3. In the Add Virtual Directory dialog box, in Alias, type CRLD. Next to Physical path, click the ellipsis "…" button.
4. In the Browse for Folder dialog box, click Local Disk (C:), and click Make New Folder.
5. Type `CRLDist`, and then press Enter. In the Browse for Folder dialog box, click OK.
6. Click OK in the Add Virtual Directory dialog box.
7. In the middle pane of the console, double-click Directory Browsing.
8. In the details pane, click Enable.
9. In the console tree, click the CRLD folder.
10. In the middle pane of the console, double-click the Configuration Editor icon.
11. Click the down-arrow for the Section drop-down list, and then navigate to system.webServer\security\requestFiltering.
12. In the middle pane of the console, double-click the allowDoubleEscaping entry to change the value from False to True.
13. In the details pane, click Apply.

Configuring the HTTPS security binding

1. Click Default Web site.
2. In the Actions pane, click Bindings.
3. In the Site Bindings dialog box, click Add.
4. In the Add Site Binding dialog box, in the Type list, click https. In SSL Certificate, click the certificate with the name app1.corp.satie.com. Click OK, and click Close.
5. Close the Internet Information Services (IIS) Manager console.

Configuring permissions on the CRL distribution point file share

1. On APP1, click Start, and click Computer.
2. Double-click Local Disk (C:).
3. In the details pane of Windows Explorer, right-click the CRLDist folder, and click Properties.
4. In the CRLDist Properties dialog box, click the Sharing tab, and then click Advanced Sharing.
5. In the Advanced Sharing dialog box, select Share this folder.

6. In Share name, add a `$`to the end so that the share name is CRLDist$.
7. In the Advanced Sharing dialog box, click Permissions.
8. In the Permissions for CRLDist$ dialog box, click Add.
9. In the Select Users, Computers, Service Accounts, or Groups dialog box, click Object Types.
10. In the Object Types dialog box, select Computers, and click OK.
11. In the Select Users, Computers, Service Accounts, or Groups dialog box, in Enter the object names to select, type `DC1`, and click Check Names. Click OK.
12. In the Permissions for CRLDist$ dialog box, select DC1 (CORP\DC1$) from the Group or user names list. In the Permissions for DC1 section, select Allow for Full control. Click OK.
13. In the Advanced Sharing dialog box, click OK.
14. In the CRLDist Properties dialog box, click the Security tab.
15. On the Security tab, click Edit.
16. In the Permissions for CRLDist dialog box, click Add.
17. In the Select Users, Computers, Service Accounts, or Groups dialog box, click Object Types.
18. In the Object Types dialog box, select Computers. Click OK.
19. In the Select Users, Computers, Service Accounts, or Groups dialog box, in Enter the object names to select, type `DC1`, and click Check Names. Click OK.
20. In the Permissions for CRLDist dialog box, select DC1 (CORP\DC1$) from the Group or user names list. In the Permissions for DC1 section, select Allow for Full control. Click OK.
21. In the CRLDist Properties dialog box, click Close.
22. Close the Windows Explorer window.

Publishing the CRL to APP1 from DC1

1. On DC1, click Start→Administrative Tools, and click Certification Authority.
2. In the console tree, open corp-DC1-CA. Right-click Revoked Certificates→All Tasks, and click Publish.
3. In the Publish CRL dialog box, click New CRL, and click OK.
4. Click Start, type `\\APP1\CRLDist$` and press Enter.
5. In the Windows Explorer window, you should see the corp-DC1-CA and corp-DC1-CA+ files.
6. Close the Windows Explorer window.
7. Close the Certification Authority console.

Creating a shared folder on APP1

1. On APP1, click Start, and click Computer.
2. Double-click Local Disk (C:).
3. Click New Folder, type `Files`, and press Enter. Leave the Local Disk window open.
4. Click Start→All Programs→Accessories, right-click Notepad, and click Run as administrator.
5. In the Untitled – Notepad window, type `This is a shared file.`
6. Click File, click Save, double-click Computer, double-click Local Disk (C:), and double-click the Files folder.
7. In File name, type `example.txt`, and click Save. Close the Notepad window.
8. In the Local Disk window, right-click the Files folder→Share with, and click Specific people.
9. Click Share, and click Done.
10. Close the Local Disk window.

Setting up and configuring the client (CLIENT1)

Installing Windows 7 SP1 on CLIENT1

1. Insert the x64 Windows 7 Professional install DVD.
2. At the Install Windows screen, click Install Now.
3. At the Get Important updates for installation, click Go online to get the latest updates.
4. At the Select your operating system screen, select Windows 7 Professional, and click Next.
5. At the license agreement screen, check I accept the license terms, and click Next.
6. At the Which type of installation do you want screen, choose Upgrade, and click Next.
7. At the Help protect Windows Automatically, choose Ask me later.
8. Set the correct date and time, and click Next.
9. At the Thank you screen, click Start.
10. When the installer prompts you for a user name, type `User1`. When it prompts you for a computer name, type `CLIENT1`.
11. When the installer prompts you for a password, type a strong password twice.
12. When the installer prompts you for protection settings, click Use recommended settings.
13. When the installer prompts you for your computer's current location, click Work.
14. Connect CLIENT1 to a network that has Internet access and run Windows Update to install the latest updates for Windows 7.
15. Connect CLIENT1 to the Corpnet subnet.

Installing Windows Updates on CLIENT1

We used the Windows Update feature to install the following updates:

- Security Update for Microsoft .NET Framework 4 Client Profile (KB2446708)
- Security Update for Microsoft Windows (KB2425227)
- Security Update for Microsoft Windows (KB2446710)
- Security Update for Microsoft Windows (KB2479943)
- Security Update for Microsoft Windows (KB2491683)
- Security Update for Microsoft Windows (KB2497640)
- Security Update for Microsoft Windows (KB2503658)
- Security Update for Microsoft Windows (KB2506212)
- Security Update for Microsoft Windows (KB2506223)
- Security Update for Microsoft Windows (KB2507618)
- Security Update for Microsoft Windows (KB2508272)
- Security Update for Microsoft Windows (KB2508429)
- Security Update for Microsoft Windows (KB2509553)
- Security Update for Microsoft Windows (KB2510531)
- Security Update for Microsoft Windows (KB2511455)
- Security Update for Microsoft Windows (KB2524375)
- Update for Microsoft Windows (KB971033)
- Update for Microsoft Windows (KB976902)
- Update for Microsoft Windows (KB2484033)
- Update for Microsoft Windows (KB2488113)
- Update for Microsoft Windows (KB2502285)

- Update for Microsoft Windows (KB2505438)
- Update for Microsoft Windows (KB2511250)

Joining CLIENT1 to the CORP domain

1. Click Start, right-click Computer, and click Properties.
2. On the System page, click Advanced system settings.
3. In the System Properties dialog box, click the Computer Name tab. On the Computer Name tab, click Change.
4. In the Computer Name/Domain Changes dialog box, click Domain, type `corp.satie.com`, and click OK.
5. When you are prompted for a user name and password, type the user name and password for the User1 domain account, and click OK.
6. When you see a dialog box that welcomes you to the corp.satie.com domain, click OK.
7. When you see a dialog box that prompts you to restart the computer, click OK.
8. In the System Properties dialog box, click Close. Click the button that restarts the computer.
9. After the computer restarts, log on as CORP\User1.

Verifying that CLIENT1 has a computer certificate installed

1. On CLIENT1, click Start, type `mmc`, and press Enter.
2. Click File, and click Add/Remove Snap-in.
3. Click Certificates, click Add, select Computer account, click Next, select Local computer, click Finish, and click OK.
4. In the console tree, open Certificates (Local Computer)\Personal\Certificates.
5. In the details pane, verify that a certificate with the name CLIENT1.corp.satie.com is present with Intended Purposes of Client Authentication and Server Authentication.
6. Close the console window. When you are prompted to save settings, click No.

Testing access to intranet resources

1. From the taskbar, click the Internet Explorer icon.
2. In the Welcome to Internet Explorer 8 window, click Next. In the Turn on Suggested Sites window, click No, don't turn on, and click Next. In the Choose your settings dialog box, click Use express settings, and click Finish.
3. In the toolbar, click Tools, and click Internet Options. For Home page, click Use blank, and click OK.
4. In the Address bar, type `http://app1.corp.satie.com/` and press Enter. You should see the default IIS 7 Web page for APP1.
5. Leave the Internet Explorer window open.
6. Click Start, type `\\app1\Files` and press Enter. You should see a folder window with the contents of the Files shared folder.
7. In the Files shared folder window, double-click the Example.txt file. You should see the contents of the Example.txt file.
8. Close the example.txt - Notepad and the Files shared folder windows.

SETTING UP AND CONFIGURING THE DIRECTACCESS MACHINE (EDGE1)

Installing Windows Server 2008 R2 SP1 on EDGE1

Installing the operating system on EDGE1

1. Start the installation of Windows Server 2008 R2.
2. Follow the instructions to complete the installation, specifying Windows Server 2008 R2 Enterprise Edition (full installation) and a strong password for the local Administrator account. Log on using the local Administrator account.
3. Connect EDGE1 to a network that has Internet access and run Windows Update to install the latest updates for Windows Server 2008 R2.
4. Connect one network adapter to the Corpnet subnet and the other to the Internet subnet.

Configuring TCP/IP properties on EDGE1

1. In Initial Configuration Tasks, click Configure networking.
2. In Network Connections, right-click the network connection that is connected to the Corpnet subnet, and click Rename.
3. Type `Corpnet` and press Enter.
4. Right-click Corpnet, and click Properties.
5. Click Internet Protocol Version 4 (TCP/IPv4), and click Properties.
6. Select Use the following IP address. In IP address, type `10.0.0.2`. In Subnet mask, type `255.255.255.0`.
7. Select Use the following DNS server addresses. In Preferred DNS server, type `10.0.0.1`.
8. Click Advanced, and click the DNS tab.
9. In DNS suffix for this connection, type `corp.satie.com` click OK twice, and click Close.
10. In the Network Connections window, right-click the network connection that is connected to the Internet subnet, and click Rename.
11. Type `Internet` and press Enter.
12. Right-click Internet, and click Properties.
13. Click Internet Protocol Version 4 (TCP/IPv4), and click Properties.
14. Select Use the following IP address. In IP address, type `131.107.0.2`. In Subnet mask, type `255.255.255.0`.
15. Click Advanced. On the IP Settings tab, click Add for IP Addresses. In the TCP/IP Address section, type `131.107.0.3` in IP address, in Subnet mask type `255.255.255.0`, and click Add.
16. Click the DNS tab.
17. In DNS suffix for this connection, type `isp.example.com` and click OK three times.
18. Close the Network Connections window.
19. To check network communication between EDGE1 and DC1, click Start→All Programs→Accessories →Command Prompt.
20. In the Command Prompt window, type `ping dc1.corp.satie.com`.
21. Verify that there are four responses from 10.0.0.1.
22. Close the Command Prompt window.

Joining EDGE1 to the CORP domain

1. In Initial Configuration Tasks, click Provide Computer Name and Domain.
2. In the System Properties dialog box, on the Computer Name tab, click Change.

3. In Computer Name, type `EDGE1`. In Member of, click Domain, and then type `corp.satie.com`
4. Click OK.
5. When you are prompted for a user name and password, type `User1` and its password, and click OK.
6. When you see a dialog box welcoming you to the corp.satie.com domain, click OK.
7. When you are prompted that you must restart the computer, click OK.
8. In the System Properties dialog box, click Close.
9. When you are prompted to restart the computer, click Restart Now.
10. After the computer has restarted, click Switch User, click Other User, and log on to the CORP domain with the User1 account.
11. In Initial Configuration Tasks, click Do not show this window at logon, and click Close.

Setting up and configuring the Web server, DNS, DHCP server (INET1)

Installing Windows Server 2008 R2 SP1 on INET1

1. Start the installation of Windows Server 2008 R2 Enterprise Edition.
2. Follow the instructions to complete the installation, specifying a strong password for the local Administrator account. Log on using the local Administrator account.
3. Connect INET1 to a network that has Internet access and run Windows Update to install the latest updates for Windows Server 2008 R2.
4. Connect INET1 to the Internet subnet.

Configuring TCP/IP properties on INET1

1. In Initial Configuration Tasks, click Configure networking.
2. In the Network Connections window, right-click Local Area Connection, and click Properties.
3. Click Internet Protocol Version 4 (TCP/IPv4), and click Properties.
4. Select Use the following IP address. In IP address, type `131.107.0.1`. In Subnet mask, type `255.255.255.0`.
5. Click Advanced, and click the DNS tab.
6. In DNS suffix for this connection, type `isp.example.com` and click OK.
7. Click OK, and click Close to close the Local Area Connection Properties dialog box.
8. Close the Network Connections window.
9. To check network communication between INET1 and EDGE1, click Start→All Programs→Accessories →Command Prompt.
10. In the Command Prompt window, type ping `131.107.0.2`
11. Verify that there are four failures from 131.107.0.2 indicating that the request timed out. The reason is that Windows Firewall with Advanced Security on EDGE1 blocks the incoming ping messages. At the command prompt, run the `arp -g command` and confirm that a Physical Address is associated with the Internet Address of 131.107.0.2. This confirms reachability to 131.107.0.2.
12. Close the Command Prompt window.
13. Click Start, right-click Network, and click Properties.
14. In the Network and Sharing Center window, click Change advanced sharing settings.
15. In the Advanced sharing settings window, click Turn on file and printer sharing, and click Save changes.
16. Close the Network and Sharing Center window.

Renaming the computer to INET1

1. In Initial Configuration Tasks, click Provide Computer Name and Domain.

2. In the System Properties dialog box, on the Computer Name tab, click Change.
3. In Computer Name, type `INET1`
4. Click OK.
5. When you are prompted that you must restart the computer, click OK.
6. On the System Properties dialog box, click Close.
7. When you are prompted to restart the computer, click Restart Now.
8. After the computer has restarted, log on with the local Administrator account.
9. In Initial Configuration Tasks, click Do not show this window at logon, and click Close.

Installing the IIS and DNS server roles on INET

1. In Server Manager, under Roles Summary, click Add Roles, and click Next.
2. On the Select Server Roles page, select Web Server (IIS) and DNS Server, and click Next.
3. Click Next twice to accept the default Web server settings, and click Install.
4. Verify that all installations were successful, and click Close.

Creating DNS records on INET

1. Click Start→Administrative Tools, and click DNS.
2. In the console tree of DNS Manager, open INET1.
3. Right-click Forward Lookup Zones, click New Zone, and click Next.
4. On the Zone Type page, click Next.
5. On the Zone Name page, type `isp.example.com` and click Next.
6. On the Dynamic Update page, click Next, and click Finish.
7. In the console tree, right-click isp.example.com, and click New Host (A or AAAA).
8. In Name, type `INET1`. In IP address, type `131.107.0.1`. Click Add Host.
9. Click OK, and click Done.
10. In the console tree, right-click Forward Lookup Zones, click New Zone, and click Next.
11. On the Zone Type page, click Next.
12. On the Zone Name page, type `satie.com` and click Next.
13. On the Dynamic Update page, click Next, and click Finish.
14. In the console tree, right-click satie.com, and click New Host (A or AAAA).
15. In Name, type EDGE1. In IP address, type `131.107.0.2`
16. Click Add Host. Click OK, and click Done.
17. In the console tree, right-click Forward Lookup Zones, click New Zone, and click Next.
18. On the Zone Type page, click Next.
19. On the Zone Name page, type `msftncsi.com` and click Next.
20. On the Dynamic Update page, click Next, and click Finish.
21. In the console tree, right-click msftncsi.com, and click New Host (A or AAAA).
22. In Name, type www. In IP address, type `131.107.0.1`
23. Click Add Host. Click OK.
24. In Name, type `dns`. In IP address, type `131.107.255.255`. Click OK, and click Done.
25. Close the DNS console.

Installing and configuring the DHCP server role

1. Click Start→Administrative Tools, and click Server Manager.
2. Under Roles Summary, click Add roles, and click Next.

3. On the Select Server Roles page, select DHCP Server, and click Next twice.
4. On the Select Network Connection Bindings page, verify that 131.107.0.1 is selected, and click Next.
5. On the Specify IPv4 DNS Server Settings page, in Parent domain, type `isp.example.com`
6. Under Preferred DNS server IP address, type `131.107.0.1`, and click Validate. Verify that the result returned is Valid, and click Next.
7. On the Specify WINS Server Settings page, accept the default setting of WINS is not required on this network, and click Next.
8. On the Add or Edit DHCP Scopes page, click Add.
9. In the Add Scope dialog box, in Scope Name, type `Internet`. In Starting IP Address, type `131.107.0.100`. In Ending IP Address, type `131.107.0.150`. In Subnet Mask, type `255.255.255.0`. In Default gateway (optional), type `131.107.0.1`.
10. Select Activate this scope, click OK, and click Next.
11. On the Configure DHCPv6 Stateless Mode page, select Disable DHCPv6 stateless mode for this server, and click Next.
12. On the Confirm Installation Selections page, click Install.
13. Verify that the installation was successful, and click Close.

Configuring the NCSI web site

1. On INET1, click Start→Computer, and navigate to C:\inetpub\wwwroot.
2. In the details pane, right-click an empty area→New, and click Text Document.
3. Rename the document to `ncsi`
4. Double-click ncsi.
5. In the Notepad window, type `Microsoft NCSI`. Do not press Enter to add a new line.
6. Click File, and click Exit. In the Notepad dialog box, click Save.

Testing access to Internet resources from the Internet subnet

1. Move CLIENT1 from Corpnet subnet to the Internet subnet. Note that after network detection is complete, the warning symbol on the network icon in the system notification area no longer appears. Hover over the network icon in the system notification area and notice that it indicates Internet access.
2. From the taskbar, click the Internet Explorer icon.
3. In the Address bar, type `http://inet1.isp.example.com/` and press Enter. You should see the default IIS 7 Web page.
4. Close the Internet Explorer window.
5. Open a command prompt window. Type `ping inet1` and press Enter. You should see four responses from 131.107.0.1. Type `ping EDGE1.satie.com` and press Enter. You should see four failures from 131.107.0.2 indicating that the request timed out. Recall that Windows Firewall with Advanced Security on EDGE1 blocks the ping messages. At the command prompt, run the `arp –g` command and confirm that a Physical Address is associated with the Internet Address of 131.107.0.2.
6. Move CLIENT1 from the Internet subnet to the Corpnet subnet.
7. From the command prompt window, type `ping inet1` and press ENTER. You should see a “could not find host inet1” message and no responses. Type ping `131.107.0.1` and press Enter. You should see “transmit failed” messages and no responses. This indicates that there is no connectivity between the Corpnet subnet and the Internet subnet.

EDGE1

Creating a DNS A record on DC1

1. Click Start→Administrative Tools, and click DNS.
2. In the console tree of DNS Manager, open DC1\corp.satie.com.
3. Right click corp.satie.com, and click New Host (A or AAAA).
4. In Name, type `nls`. In IP address, type `10.0.0.3`. Click Add Host, click OK, and click Done.
5. Close the DNS Manager console.

Creating a security group for DirectAccess client computers on DC1

1. In the Active Directory Users and Computers console tree, right-click Users→New, and click Group.
2. In the New Object - Group dialog box, under Group name, type `DA_Clients`
3. Under Group scope, choose Global, under Group type, choose Security, and click OK.
4. In the details pane, double-click DA_Clients.
5. In the DA_Clients Properties dialog box, click the Members tab, and click Add.
6. In the Select Users, Contacts, Computers, or Groups dialog box, click Object Types, click Computers, and click OK.
7. Under Enter the object names to select (examples), type `CLIENT1` and click OK.
8. Verify that CLIENT1 is displayed below Members, and click OK.
9. Close the Active Directory Users and Computers console.

Configuring permissions of the Web Server certificate template on DC1

1. Click Start, type `certtmpl.msc` and press Enter.
2. In the contents pane, right-click the Web Server template, and click Properties.
3. Click the Security tab, and click Authenticated Users.
4. In Permissions for Authenticated Users, click Enroll under Allow, and click OK. Note: The Authenticated Users group is configured here for simplicity in the test lab. In a real deployment, you would specify the name of a security group that contains the computer accounts of the computers in your organization that can request custom certificates, which includes the DirectAccess server and network location server.
5. Close the Certificate Templates console.

Creating and enabling firewall rules for ICMPv6 traffic

1. Click Start→Administrative Tools→Group Policy Management.
2. In the console tree, open Forest: Satie.com\Domains\corp.satie.com.
3. In the console tree, right-click Default Domain Policy, and click Edit.
4. In the console tree of the Group Policy Management Editor, open Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security.
5. In the console tree, right-click Inbound Rules, and click New Rule.
6. On the Rule Type page, click Custom, and click Next.
7. On the Program page, click Next.
8. On the Protocols and Ports page, for Protocol type, click ICMPv6, and then click Customize.
9. In the Customize ICMP Settings dialog box, click Specific ICMP types, select Echo Request, and click OK.
10. Click Next.
11. On the Scope page, click Next.

12. On the Action page, click Next.
13. On the Profile page, click Next.
14. On the Name page, for Name, type `Inbound ICMPv6 Echo Requests` and click Finish.
15. In the console tree, right-click Outbound Rules, and click New Rule.
16. On the Rule Type page, click Custom, and click Next.
17. On the Program page, click Next.
18. On the Protocols and Ports page, for Protocol type, click ICMPv6, and click Customize.
19. In the Customize ICMP Settings dialog box, click Specific ICMP types, select Echo Request, and click OK.
20. Click Next.
21. On the Scope page, click Next.
22. On the Action page, click Allow the connection, and click Next.
23. On the Profile page, click Next.
24. On the Name page, for Name, type `Outbound ICMPv6 Echo Requests` and click Finish.
25. Close the Group Policy Management Editor and Group Policy Management consoles.

Removing ISATAP from the DNS global query block list

1. Click Start→All Programs→Accessories, right-click Command Prompt, and click Run as administrator.
2. In the Command Prompt window, type `dnscmd /config /globalqueryblocklist wpad` and press Enter.
3. Close the Command Prompt window.

Configuring additional CRL distribution settings

1. Click Start→Administrative Tools, and click Certification Authority.
2. In the console tree, right-click corp-DC1-CA, and click Properties.
3. Click the Extensions tab, and click Add.
4. In Location, type `http://crl.satie.com/crld/`
5. In Variable, click <CAName>, and click Insert.
6. In Variable, click <CRLNameSuffix>, and click Insert.
7. In Variable, click <DeltaCRLAllowed>, and click Insert.
8. In Location, type `.crl` at the end of the Location string, and click OK.
9. Select Include in CRLs. Clients use this to find Delta CRL locations. and Include in the CDP extension of issued certificates, and click OK.
10. Click Add.
11. In Location, type `\\EDGE1\crldist$\`
12. In Variable, click <CAName>, and click Insert.
13. In Variable, click <CRLNameSuffix>, and click Insert.
14. In Variable, click <DeltaCRLAllowed>, and click Insert.
15. In Location, type `.crl` at the end of the string, and click OK.
16. Select Publish CRLs to this location and Publish Delta CRLs to this location, and click OK.
17. Click Yes to restart Active Directory Certificate Services.
18. Close the Certification Authority console.

Installing the IIS server role on EDGE1

1. In the console tree of Server Manager, click Roles. In the details pane, click Add Roles, and click Next.
2. On the Select Server Roles page, click Web Server (IIS), and click Next three times.

3. Click Install.
4. Verify that all installations were successful, and click Close.
5. Leave the Server Manager window open.

Creating a Web-based CRL distribution point on EDGE1

1. Click Start→Administrative Tools, and click Internet Information Services (IIS) Manager.
2. In the console tree, open EDGE1, and then Sites.
3. Right-click Default Web Site, and click Add virtual directory.
4. In Alias, type `CRLD`
5. In Physical path, click the ellipsis (…).
6. Click the drive on which Windows Server 2008 R2 is located, and click Make New Folder.
7. Type `CRLDist` press Enter, and click OK twice.
8. In the Contents pane, double-click Directory Browsing.
9. In the Actions pane, click Enable.
10. In the console tree, click the CRLD folder.
11. In the Contents pane, double-click Configuration Editor.
12. In Section, open system.webServer\security\requestFiltering.
13. In the Contents pane, double-click allowDoubleEscaping to change it from False to True.
14. In the Actions pane, click Apply.
15. Close the Internet Information Services (IIS) Manager window.

Configuring permissions on the CRLDist file share

1. Click Start→Computer.
2. Double-click the drive on which Windows Server 2008 R2 is located.
3. In the Details pane, right-click the CRLDist folder, and click Properties.
4. Click the Sharing tab, and click Advanced Sharing.
5. Select Share this folder.
6. In Share name, add `$` to the end of the CRLDist name to hide the share, and click Permissions.
7. Click Add, and click Object Types.
8. Select Computers, and click OK.
9. In Enter the object names to select, type `DC1` and click OK.
10. In Group or user names, click the DC1 computer. In Permissions for DC1, click Full Control, and click OK twice.
11. Click the Security tab, and click Edit.
12. Click Add, and click Object Types.
13. Select Computers, and click OK.
14. In Enter the object names to select, type `DC1` and click OK.
15. In Group or user names, click the DC1 computer. In Permissions for DC1, click Full Control, click OK, and click Close.
16. Close the Local Disk window.

Publishing the CRL on EDGE1

1. On DC1, click Start→Administrative Tools, and click Certification Authority.
2. In the console tree, double-click corp-DC1-CA, right-click Revoked Certificates→All Tasks, and click Publish.

3. If prompted, click New CRL, and click OK.
4. Click Start, type `\\EDGE1\crldist$` and press Enter.
5. In the crldist$ window, you should see two CRL files named corp-DC1-CA and corp-DC1-CA+.
6. Close the crldist$ window and the Certification Authority console.

Obtaining an additional certificate for EDGE1

1. On EDGE1, click Start, type `mmc` and press Enter. Click Yes at the User Account Control prompt.
2. Click File, and click Add/Remove Snap-ins.
3. Click Certificates, click Add, click Computer account, click Next, select Local computer, click Finish, and click OK.
4. In the console tree of the Certificates snap-in, open Certificates (Local Computer)\Personal\Certificates.
5. Right-click Certificates→All Tasks, and click Request New Certificate.
6. Click Next twice.
7. On the Request Certificates page, click Web Server, and then click More information is required to enroll for this certificate.
8. On the Subject tab of the Certificate Properties dialog box, in Subject name, for Type, select Common Name.
9. In Value, type `EDGE1.satie.com` and click Add.
10. Click OK, click Enroll, and click Finish.
11. In the Details pane of the Certificates snap-in, verify that a new certificate with the name EDGE1.satie.com was enrolled with Intended Purposes of Server Authentication.
12. Right-click the certificate, and click Properties.
13. In Friendly Name, type `IP-HTTPS Certificate` and click OK.
14. Close the console window. If you are prompted to save settings, click No.

Obtaining an additional certificate for APP1

1. Click Start, type `mmc` and press Enter.
2. Click File, and click Add/Remove Snap-in.
3. Click Certificates, click Add, select Computer account, click Next, select Local computer, click Finish, and click OK.
4. In the console tree of the Certificates snap-in, open Certificates (Local Computer)\Personal\Certificates.
5. Right-click Certificates→All Tasks, and click Request New Certificate.
6. Click Next twice.
7. On the Request Certificates page, click Web Server, and click More information is required to enroll for this certificate.
8. On the Subject tab of the Certificate Properties dialog box, in Subject name, for Type, select Common Name.
9. In Value, type `nls.corp.satie.com` and click Add.
10. Click OK, click Enroll, and click Finish.
11. In the details pane of the Certificates snap-in, verify that a new certificate with the name nls.corp.satie.com was enrolled with Intended Purposes of Server Authentication.
12. Close the console window. If you are prompted to save settings, click No.

Configuring the HTTPS security binding on APP1

1. Click Start→Administrative Tools, and click Internet Information Services (IIS) Manager.
2. In the console tree of Internet Information Services (IIS) Manager, open APP1/Sites, and click Default Web site.
3. In the Actions pane, click Bindings.
4. In the Site Bindings dialog box, click Add.
5. In the Add Site Binding dialog box, in the Type list, click https. In SSL Certificate, click the certificate with the name nls.corp.satie.com. Click OK, and click Close.
6. Close the Internet Information Services (IIS) Manager console.

Creating an A record

1. Click Start→Administrative Tools, and click DNS.
2. In the console tree, right click satie.com, and click New Host (A or AAAA).
3. In Name, type `crl`. In IP address, type `131.107.0.2`
4. Click Add Host. Click OK, and click Done.
5. Close the DNS console.

Installing Windows 7 on NAT1

1. Start the installation of x64 Windows 7 Professional.
2. When the installer prompts you for a user name, type `User1`. When the installer prompts you for a computer name, type `NAT1`
3. When the installer prompts you for a password, type a strong password twice.
4. When the installer prompts you for protection settings, click Use recommended settings.
5. When the installer prompts you for your computer's current location, click Public.
6. After installation, connect NAT1 to a network that has access to the Internet and run Windows Update and apply the following.
    - Security Update for Microsoft .NET Framework 4 Client Profile (KB2446708)
    - Security Update for Microsoft Windows (KB2425227)
    - Security Update for Microsoft Windows (KB2446710)
    - Security Update for Microsoft Windows (KB2479943)
    - Security Update for Microsoft Windows (KB2491683)
    - Security Update for Microsoft Windows (KB2497640)
    - Security Update for Microsoft Windows (KB2503658)
    - Security Update for Microsoft Windows (KB2506212)
    - Security Update for Microsoft Windows (KB2506223)
    - Security Update for Microsoft Windows (KB2507618)
    - Security Update for Microsoft Windows (KB2508272)
    - Security Update for Microsoft Windows (KB2508429)
    - Security Update for Microsoft Windows (KB2509553)
    - Security Update for Microsoft Windows (KB2510531)
    - Security Update for Microsoft Windows (KB2511455)
    - Security Update for Microsoft Windows (KB2524375)
    - Update for Microsoft Windows (KB971033)
    - Update for Microsoft Windows (KB976902)

- Update for Microsoft Windows (KB2484033)
- Update for Microsoft Windows (KB2488113)
- Update for Microsoft Windows (KB2502285)
- Update for Microsoft Windows (KB2505438)
- Update for Microsoft Windows (KB2511250)

7. Connect one network adapter to the Internet subnet and the other network adapter to the Homenet subnet.

Configuring Network Connections properties on NAT1

1. Click Start→Control Panel.
2. Under Network and Internet, click View status and tasks, and click Change adapter settings.
3. In the Network Connections window, right-click the network connection that is connected to the Homenet subnet, and click Rename.
4. Type `Homenet` and press Enter.
5. In the Network Connections window, right-click the network connection that is connected to the Internet subnet, and click Rename.
6. Type `Internet` and press Enter.
7. Leave the Network Connections window open for the next procedure.
8. Click Start→All Programs→Accessories, right-click Command Prompt, and click Run as administrator.
9. To check network communication between NAT1 and INET1, in the Command Prompt window, type `ping inet1.isp.example.com` and press Enter.
10. Verify that there are four responses from 131.107.0.1.
11. In the Command Prompt window, type `netsh interface 6to4 set state state=disabled` and press Enter.
12. Close the Command Prompt window.

Configuring Internet Connection Sharing on NAT1

1. In the Network Connections window, right-click Internet, and click Properties.
2. Click the Sharing tab, select Allow other network users to connect through this computer's Internet connection, and click OK.

Testing access to the network location server from CLIENT1

1. From the taskbar, click the Internet Explorer icon.
2. In the Address bar, type `https://nls.corp.satie.com` and press Enter. You should see the default IIS 7 Web page.
3. Close Internet Explorer.

Installing the DirectAccess feature on EDGE1 from Server Manager

1. Log onto EDGE1 with the User1 user account and password.
2. Click Start→Administrative Tools, and click Server Manager.
3. In the main window, under Features Summary, click Add features
4. On the Select Features page, select DirectAccess Management Console.
5. In the Add Features Wizard window, click Add Required Features.
6. On the Select Features page, click Next.
7. On the Confirm Installation Selections page, click Install.
8. On the Installation Results page, click Close.

Running the DirectAccess Setup Wizard

1. Click Start→Administrative Tools, and click DirectAccess Management.
2. In the console tree, click Setup. In the Details pane, click Configure for step 1.
3. On the DirectAccess Client Setup page, click Add.
4. In the Select Group dialog box, type `DA_Clients` click OK, and click Finish.
5. Click Configure for step 2.
6. On the Connectivity page, for Interface connected to the Internet, select Internet. For Interface connected to the internal network, select Corpnet. Click Next.
7. On the Certificate Components page, for Select the root certificate to which remote client certificates must chain, click Browse. In the list of certificates, click the corp-DC1-CA root certificate, and click OK.
8. For Select the certificate that will be used to secure remote client connectivity over HTTPS, click Browse. In the list of certificates, click the certificate named IP-HTTPS Certificate, and click OK. Click Finish.
9. Click Configure for step 3.
10. On the Location page, click Network Location server is run on a highly available server, type `https://nls.corp.satie.com` click Validate, and click Next.
11. On the DNS and Domain Controller page, note the entry for the name corp.satie.com with the IPv6 address 2002:836b:2:1:0:5efe:10.0.0.1. This IPv6 address is assigned to DC1 and is composed of a 6to4 network prefix (2002:836b:2:1::/64) and an ISATAP-based interface identifier (::0:5efe:10.0.0.1). Click Next.
12. On the Management page, click Finish.
13. Click Configure for step 4. On the DirectAccess Application Server Setup page, click Finish.
14. Click Save, and click Finish.
15. In the DirectAccess Review dialog box, click Apply. In the DirectAccess Policy Configuration message box, click OK.

Updating IPv6 settings on APP1

1. On APP1, click Start→All Programs→Accessories, right-click Command Prompt, and click Run as administrator.
2. From the Command Prompt window, type `net stop iphlpsvc` and press Enter, and type `net start iphlpsvc` and press Enter.
3. Close the Command Prompt window.

Updating IPv6 settings on DC1

1. On DC1, click Start→All Programs→Accessories, right-click Command Prompt, and click Run as administrator.
2. From the Command Prompt window, type `net stop iphlpsvc` and press Enter, and type `net start iphlpsvc` and press Enter.
3. Close the Command Prompt window.

Updating Group Policy and IPv6 settings on CLIENT1

1. On CLIENT1, click Start→All Programs→Accessories, right-click Command Prompt, and click Run as administrator.
2. From the Command Prompt window, type `gpupdate` and press Enter.

3. From the Command Prompt window, type `net stop iphlpsvc` and press Enter, and type `net start iphlpsvc` and press Enter.
4. Leave the Command Prompt window open for the next procedure.

Verifying ISATAP-based connectivity to DC1 and APP1

1. On CLIENT1, from the Command Prompt window, type `ipconfig /flushdns` and press Enter.
2. From the Command Prompt window, type `ping 2002:836b:2:1::5efe:10.0.0.1` and press Enter. This is the ISATAP-based address of DC1. You should see four successful replies.
3. From the Command Prompt window, type `ping 2002:836b:2:1::5efe:10.0.0.3` and press Enter. This is the ISATAP-based address of APP1. You should see four successful replies.
4. From the Command Prompt window, `type ping dc1.corp.satie.com` and press Enter. You should see the name dc1.corp.satie.com resolved to the IPv6 address 2002:836b:2:1::5efe:10.0.0.1 and four successful replies.
5. From the Command Prompt window, type `ping app1.corp.satie.com` and press Enter. You should see the name app1.corp.satie.com resolved to the IPv6 address 2002:836b:2:1::5efe:10.0.0.3 and four successful replies.
6. Leave the Command Prompt window open for the next procedure.

Connecting CLIENT1 to the Internet subnet

1. Unplug the Ethernet cable of CLIENT1 from the switch for the Corpnet subnet and then plug it into the switch for the Internet subnet. Wait until the network icon in the notification area of the desktop displays a connected network.
2. To verify that the proper IPv4 address has been configured, from the Command Prompt window, type `ipconfig` and press Enter.
3. In the display of the Ipconfig.exe tool, verify that the interface named Local Area Connection has an IPv4 address that begins with 131.107.
4. Leave the Command Prompt window open for the next procedure.

Verifying connectivity to Internet resources

1. From the Command Prompt window, type `ping inet1.isp.example.com` and press Enter.
2. You should see the name inet1.isp.example.com resolved to the IPv4 address 131.107.0.1 and four successful replies.
3. From the taskbar, click the Internet Explorer icon.
4. In the Address bar, type `http://inet1.isp.example.com/` and press Enter. You should see the default IIS 7 Web page for INET1.
5. Leave the Internet Explorer window open for the next procedure.

Verifying that CLIENT1 can access intranet resources

1. From the Command Prompt window, type `ping app1` and press Enter.
2. You should see the name app1.corp.satie.com resolved to the IPv6 address 2002:836b:2:1:0:5efe:10.0.0.3 and four successful replies.
3. In Internet Explorer, in the Address bar, type `http://app1.corp.satie.com/` press Enter, and press F5. You should see the default IIS 7 Web page for APP1.
4. Close Internet Explorer.
5. Click Start, type `\\app1\files` and press Enter. You should see a folder window with the contents of the Files shared folder.

6. In the Files shared folder window, double-click the Example.txt file.
7. Close the example.txt - Notepad window and the Files shared folder window.
8. Examine CLIENT1's IPv6 configuration.
9. From the Command Prompt window, type `ipconfig` and press ENTER.
10. From the display of the Ipconfig.exe tool, notice that an interface named Tunnel adapter 6TO4 Adapter has an IPv6 address that begins with 2002:836b:. This is a 6to4 address based on an IPv4 address that begins with 131.107.

Connecting CLIENT1 to the Homenet subnet

1. Unplug the Ethernet cable of CLIENT1 from the switch for the Internet subnet and then plug it into the switch for the Homenet subnet. Wait until the network icon in the notification area of the desktop displays a connected network.
2. To verify that the proper IPv4 address has been configured, from the Command Prompt window, type `ipconfig` and press Enter.
3. In the display of the Ipconfig.exe tool, verify that the interface named Local Area Connection has an IPv4 address starting with 192.168.137.
4. Leave the Command Prompt window open for the next procedure.

Verifying connectivity to Internet resources

1. From the Command Prompt window, type `ping inet1.isp.example.com` and press Enter.
2. You should see the name inet1.isp.example.com resolved to the IPv4 address 131.107.0.1 and four successful replies.
3. In the task bar, click the Internet Explorer icon.
4. In the Address bar, type `http://inet1.isp.example.com/` press Enter, and press F5. You should see the default IIS 7 Web page for INET1.
5. Leave the Internet Explorer window open for the next procedure.

Verifying that CLIENT1 can access intranet resources

1. In the Address bar of Internet Explorer, type `http://app1.corp.satie.com/` and press Enter. You should see the default IIS 7 Web page for APP1.
2. Close Internet Explorer.
3. Click Start, type `\\app1\files` and press Enter.
4. You should see a folder window with the contents of the Files shared folder.
5. In the Files shared folder window, double-click the Example.txt file.
6. Close the example.txt - Notepad window and the Files shared folder window.

Examining the CLIENT1 IPv6 configuration

1. From the Command Prompt window, type `ipconfig` and press Enter.
2. From the display of the Ipconfig.exe tool, notice that an interface has an IPv6 address that starts with 2001:. This is a Teredo address assigned by EDGE1. When CLIENT1 is behind a NAT that does not support 6to4 router functionality, CLIENT1 uses Teredo to tunnel IPv6 traffic to EDGE1.
3. Leave the Command Prompt window open for the next procedure.

Disabling Teredo connectivity on CLIENT1

1. From the Command Prompt window, type `netsh interface teredo set state disabled` and press Enter.

2. Unplug the Ethernet cable of CLIENT1 from the switch for the Homenet subnet and then plug it back into the switch for the Homenet subnet. Wait until the network icon in the notification area of the desktop displays a connected network.
3. From the Command Prompt window, type `ipconfig` and press Enter.
4. In the display of the Ipconfig.exe tool, verify that there is an interface named IPHTTPSinterface with an IPv6 address that starts with 2002:836b:2:2. This is an address assigned to the IP-HTTPS interface by EDGE1. When CLIENT1 is behind a Web proxy or firewall that does not forward Teredo traffic, CLIENT1 uses IP-HTTPS to tunnel IPv6 traffic to EDGE1.
5. Leave the Command Prompt window open for the next procedure.

Verifying that CLIENT1 can access intranet resources

1. In the Address bar, type `http://app1.corp.satie.com/` press Enter, and press F5. You should see the default IIS 7 Web page for APP1.
2. Close Internet Explorer.
3. Click Start, type `\\app1\files` and press Enter.
4. You should see a folder window with the contents of the Files shared folder.
5. In the Files shared folder window, double-click the Example.txt file.
6. Close the example.txt - Notepad window and the Files shared folder window.

Enabling Teredo connectivity on CLIENT1

1. From the Command Prompt window, type `netsh interface teredo set state enterpriseclient` and press Enter.
2. From the Command Prompt window, type `ipconfig` and press Enter.
3. In the display of the Ipconfig.exe tool, verify that an interface has an IPv6 address that starts with 2001.

Connecting CLIENT1 to the Corpnet subnet

1. Unplug the Ethernet cable of CLIENT1 from the switch for the Homenet subnet and plug it into the switch for the Corpnet subnet.
2. Log onto CLIENT1 by using the User1 account.
3. In the taskbar, click the Internet Explorer icon.
4. In the Address bar of Internet Explorer, type `http://app1.corp.satie.com/` press Enter, and press F5. You should see the default IIS 7 Web page for APP1.
5. Close Internet Explorer.
6. Click Start, type `\\app1\files` and press Enter.
7. You should see a folder window with the contents of the Files shared folder.
8. In the Files shared folder window, double-click the Example.txt file.
9. Close the example.txt - Notepad window and the Files shared folder window.

Running the test

1. Launch SYSmark 2007 Preview by double-clicking the desktop icon.
2. Click Run.
3. Select Official Run, choose 3 Iterations, check the box beside Run conditioning run, and enter a name for that run.
4. When the benchmark completes and the main SYSmark 2007 Preview menu appears, click Save FDR to create a report.
5. Record the results for each iteration.

CONFIGURING THE NETWORK INFRASTRUCTURE FOR VPN TESTING

Installing Windows Server 2008 R2 SP1 on domain controller (DC1)

Installing Windows Server 2008 R2 SP1 on DC1

1. Insert the installation DVD for Windows Server 2008 SP1 x64 into the DVD drive.
2. Choose the language, time and currency, and keyboard input. Click Next.
3. Click Install Now.
4. Choose Windows Server Enterprise (Full Installation). Click Next.
5. Accept the license terms, and click Next.
6. Click Custom.
7. Click the Disk, and click Drive options (advanced).
8. Click New, Apply, Format, and click Next.
9. Let the installation process continue. The server will reboot several times.
10. After the installation completes, click OK to set the Administrator password.
11. Enter the administrator password twice, and click OK.
12. Click Start→Control Panel, and double-click System.
13. Click Change Settings.
14. Click Change.
15. Enter the new computer name, and click OK.
16. Click OK to restart, click Close, and click Restart Now.

Installing Windows updates on DC1

We used the Windows Update feature to install the following updates:

- Windows Internet Explorer 9
- Security Update for Microsoft Windows (KB2524375)
- Security Update for Microsoft Windows (KB2511455)
- Security Update for Microsoft Windows (KB2510531)
- Security Update for Microsoft Windows (KB2509553)
- Security Update for Microsoft Windows (KB2508429)
- Security Update for Microsoft Windows (KB2508272)
- Security Update for Microsoft Windows (KB2507618)
- Security Update for Microsoft Windows (KB2506223)
- Security Update for Microsoft Windows (KB2506212)
- Security Update for Microsoft Windows (KB2506014)
- Security Update for Microsoft Windows (KB2503658)
- Security Update for Microsoft Windows (KB2497640)
- Security Update for Microsoft Windows (KB2425227)
- Security Update for Microsoft Windows (KB2446710)
- Security Update for Microsoft Windows (KB976902)

Configuring TCP/IP properties

1. After DC1 restarts, in the Initial Configuration Tasks window, under 1. Provide Computer Information**,** click Configure networking**.**
2. In the Network Connections dialog box, right-click Local Area Connection, and click Properties.

3. In the Local Area Connection Properties dialog box, click Internet Protocol Version 4 (TCP/IPv4), and click Properties.
4. Click Use the following IP address, and configure the following settings:
   a. In IP address, type `192.168.0.1`
   b. In Subnet mask, type `255.255.255.0`
   c. In Default gateway, type `191.168.0.2`
   d. In Preferred DNS server, type `192.168.0.1`
5. Click OK, and click Close.
6. Close the Network Connections window.

Installing Active Directory and DNS on DC1

1. On DC1, in the Initial Configuration Tasks window, under 3. Customize This Server, click Add roles, and perform the following steps in the Add Roles Wizard:
   a. In the Add Roles Wizard, on the Before You Begin page, click Next.
   b. On the Select Server Roles page, select Active Directory Domain Services.
   c. In the Add features required for Active Directory Domain Services dialog box, click Add Required Features.
   d. Back on the Select Server Roles page, click Next.
   e. On the Active Directory Domain Services page, click Next, and on the Confirm Installation Selections page, click Install.
   f. On the Installation Results page click Close this wizard and launch the Active Directory Services Installation Wizard (dcpromo.exe).
2. In the Active Directory Domain Services Installation Wizard, perform the following steps:
   a. On the Welcome page, click Next.
   b. On the Operating System Compatibility page, click Next.
   c. On the Choose a Deployment Configuration page, select Create a new domain in a new forest, and click Next.
   d. On the Name the Forest Root Domain page, type `satie.com` and click Next.
   e. On the Set Forest Functional Level page, select Windows Server 2008 R2, and click Next.
   f. In the Additional Domain Controller Options page, ensure that DNS server is selected, and click Next.
   g. On the notice dialog that indicates that a delegation for the DNS server cannot be created, click Yes.
   h. On the Location for Database, Log Files, and SYSVOL page, click Next.
   i. On the Directory Services Restore Mode Administrator Password page, type `Pass@word1` in both text boxes, and click Next.
   j. On the Summary page, click Next.
   k. On the progress dialog box, select Reboot on completion.
   l. On the Completing page, click Finish, and click Restart Now.

Creating a user account with remote access permission

1. After DC1 restarts, log on as Satie\Administrator
2. Click Start→Administrative Tools, and click Active Directory Users and Computers.
3. In the navigation tree, expand satie.com, right-click Users, click New, and click User.
4. In Full name, type `user1` and in User logon name, type `user1`. Click Next.
5. In Password, type `Pass@word1` and in Confirm password, type `Pass@word1` again.

6. Clear the User must change password at next logon check box, and then select the User cannot change password and Password never expires check boxes.
7. Click Next, and click Finish.

Granting remote access permission to user1:

1. In the left tree, click Users. In the details pane, double-click user1.
2. On the Dial-in tab, under Network Access Permission, click Allow access, and click OK.
3. Close Active Directory Users and Computers.

Creating a shared folder and file

1. On DC1, click Start→My Computer.
2. Double-click Local Disk (C:).
3. On the toolbar, click New folder, and type the name `CorpData`
4. Right-click the CorpData folder, click Share with, and click Specific people.
5. In the File Sharing dialog box, type `Everyone` and click Add.
6. In the list, click the entry for Everyone, and click Read/Write.
7. Click Share, and click Done to complete the process. The folder is now accessible as \\dc1\corpdata.
8. Double-click the CorpData folder, and then right-click in the blank space. Point to New, and click Text Document.
9. Name the document `VPNTest` (the .txt file type extension is added automatically).
10. Open VPNTest and add some text.
11. Save and close VPNTest.

Installing the operating system on the virtual private network server (VPN1)

Installing Windows Server 2008 R2 SP1

1. Insert the installation DVD for Windows Server 2008 SP1 x64 into the DVD drive.
2. Choose the language, time and currency, and keyboard input. Click Next.
3. Click Install Now.
4. Choose Windows Server Enterprise (Full Installation), and click Next.
5. Accept the license terms, and click Next.
6. Click Custom.
7. Click the Disk, and click Drive options (advanced).
8. Click New, Apply, Format, and click Next.
9. Let the installation process continue. The server will reboot several times.
10. After the installation completes, click OK to set the Administrator password.
11. Enter the administrator password twice, and click OK.
12. Click Start→Control Panel, and double-click System.
13. Click Change Settings.
14. Click Change.
15. Enter the new computer name, and click OK.
16. Click OK to restart, click Close, and click Restart Now.

Installing Windows updates on VPN1

We used the Windows Update feature to install the following updates:

- Windows Internet Explorer 9
- Security Update for Microsoft Windows (KB2524375)

- Security Update for Microsoft Windows (KB2511455)
- Security Update for Microsoft Windows (KB2510531)
- Security Update for Microsoft Windows (KB2509553)
- Security Update for Microsoft Windows (KB2508429)
- Security Update for Microsoft Windows (KB2508272)
- Security Update for Microsoft Windows (KB2507618)
- Security Update for Microsoft Windows (KB2506223)
- Security Update for Microsoft Windows (KB2506212)
- Security Update for Microsoft Windows (KB2506014)
- Security Update for Microsoft Windows (KB2503658)
- Security Update for Microsoft Windows (KB2497640)
- Security Update for Microsoft Windows (KB2425227)
- Security Update for Microsoft Windows (KB2446710)
- Security Update for Microsoft Windows (KB976902)

Configuring TCP/IP on VPN1

Configuring TCP/IP properties

1. On VPN1, in the Initial Configuration Tasks window, under 1. Provide Computer Information, click Configure networking.
2. In the Network Connections dialog box, right-click the connection for the adapter that is connected to the public (Internet) network, and click Properties.
3. On the Networking tab, click Internet Protocol Version 4 (TCP/IPv4), and click Properties.
4. Click Use the following IP address, and configure the following settings:
   a. In IP address, type `131.107.0.2`
   b. In Subnet mask, type `255.255.0.0`
   c. Do not configure a default gateway or DNS server on this connection.
   d. Click OK twice to return to Network Connections.
5. Right-click the connection for the adapter that is connected to the private network, and click Properties.
6. Click Use the following IP address, and configure the following settings:
   a. In IP address, type `192.168.0.2`
   b. In Subnet mask, type `255.255.255.0`
   c. Do not configure a default gateway on this connection.
   d. In Preferred DNS server, type `192.168.0.1`
   e. Click OK twice to return to Network Connections.
7. To rename the network connections, right-click a network connection, and click Rename.
8. Rename the network connections with the following names:
   a. On the interface connected to the public (Internet) network, type **`Public`**
   b. On the interface connected to the private (intranet) network, type **`Private`**
9. Close the Network Connections window.

Use the ping command to verify network connectivity between VPN1 and DC1, and to verify that VPN1 can use DC1 for name resolution.

Using the ping command to check network connectivity

1. On VPN1, click Start, click Run, in the Open box, type **`cmd`** and click OK. In the Command Prompt window, type **`ping dc1`**
2. Verify that you can successfully ping DC1.
3. Close the Command Prompt window.

Naming the computer and join the domain

1. On VPN1, in the Initial Configuration Tasks window, under 1. Provide Computer Information, click Provide computer name and domain.
2. In the System Properties dialog box, on the Computer Name tab, click Change.
3. In Computer name, clear the text and type `VPN1`
4. In Member of, click Domain, type `satie` and click OK.
5. Enter administrator for the user name and `Pass@word1` for the password.
6. When you see a dialog box welcoming you to the satie.com domain, click OK.
7. When you see a dialog box telling you to restart the computer, click OK. Click Close, and click Restart Now.

Installing Active Directory Certificate Services and Web Server

1. After VPN1 restarts, log on as satie\administrator with the password Pass@word1.
2. In the Initial Configuration Tasks window, under 3. Customize This Server, click Add roles.
3. In the Add Roles Wizard dialog box, on the Before You Begin page, click Next.
4. On the Select Server Roles page, select Active Directory Certificate Services, and click Next.
5. On the Introduction to Active Directory Certificate Services page, click Next.
6. On the Select Role Services page, select both Certification Authority and Certification Authority Web Enrollment.
7. In the Add role services and features required for Certification Authority Web Enrollment dialog box, click Add Required Role Services.
8. Click Next.
9. On the Specify Setup Type, select Enterprise, and click Next.
10. On the Specify CA Type page, select Root CA, and click Next.
11. On the Set Up Private Key page, select Create a new private key, and click Next.
12. On the Configure Cryptography for CA page, click Next to accept the default cryptographic settings.
13. On the Configure CA Name page, click Next to accept the default CA common name and suffix.
14. On the Set Validity Period page, click Next to accept the default validity period.
15. On the Configure Certificate Database page, click Next to accept the default locations.
16. On the Web Server (IIS) page, click Next.
17. On the Select Role Services page, click Next to accept the default choices.
18. In the Confirm Installation Selections dialog box, click Install. The installation might take several minutes.
19. In the Installation Results dialog box, click Close.

Creating and installing the Server Authentication certificate

1. On VPN1, click Start→Administrative Tools, and click Certification Authority.
2. In the navigation tree, expand satie-VPN1-CA.
3. Right-click Certificate Templates, and then click Manage. The Certificate Templates Console appears.

4. Right-click the IPsec template in the list, and then click Duplicate Template.
5. In the Duplicate Template dialog box, select Windows Server 2003 Enterprise, and click OK.
6. On the General tab, change the Template display name to VPN Reconnect.
7. Check the Validity period. The default is 2 years, but you can adjust this per your organization's requirements.
8. On the Request Handling tab, select Allow private key to be exported.
9. On the Subject Name tab, select Supply in the request. If a warning message appears, click OK.
10. On the Extensions tab, select Application Policies, and click Edit.
11. The IP security IKE intermediate policy is already present. Keep it. If there are any others, select them and click Remove.
12. Click Add, select Server Authentication, and click OK.
13. Click OK to return to the Extensions tab.
14. Select Key Usage, and click Edit.
15. In the Signature section, ensure that Digital signature is selected. If it is, click Cancel. If it is not, select it, and click OK.
16. Click OK to save your completed template.
17. Close the Certificate Templates Console window.
18. The certificate template has been created. It must be issued before it can be used to request a certificate.

Issuing the certificate template

1. In the Certification Authority console window, right-click Certificate Templates, click New, and click Certificate Template to Issue.
2. In the Enable Certificate Templates dialog box, select VPN Reconnect, and click OK.

The template is now ready to be used for certificate requests. Before you can request one, you must configure Internet Explorer security settings to work with the certificate publishing Web page.

Configuring Internet Explorer to allow certificate publishing

1. On VPN1, click Start, right-click Internet Explorer, and click Run as administrator.
2. Click Tools, and click Internet Options.
3. On the Security tab, under Select a zone to view or change security settings, click Local intranet.
4. Change the security level for Local intranet from Medium-low to Low, and click OK.

Requesting a Server Authentication certificate using Internet Explorer

1. On VPN1, in the Internet Explorer address bar, type `http://localhost/certsrv` and press Enter.
2. Under Select a Task, click Request a Certificate.
3. Under Request a Certificate, click Advanced Certificate Request.
4. Under Advanced Certificate Request, click Create and submit a request to this CA.
5. On the first confirmation dialog box, click Yes to allow the ActiveX control.
6. On the second confirmation dialog box, click Yes to allow the certificate operation.
7. In the Certificate Template list, select VPN Reconnect.
8. Under Identifying Information, in the Name field, type `vpn1.satie.com`
9. Under Key Options, select Mark keys as exportable, and click Submit.
10. Click Yes in each of the confirmation dialog boxes.

The server authentication certificate is created in the user personal store. It must be moved to the machine store to be used.

Moving the certificate to the machine store

1. On VPN1, click Start, type `MMC` and press Enter.
2. In Console1, click File, and click Add/Remove Snap-in.
3. Under Available snap-ins, click Certificates, and click Add.
4. Click Finish to accept the default setting of My user account.
5. Click Add a second time, click Computer account, and click Next.
6. In the Select Computer dialog box, click Finish to accept the default setting of Local computer.
7. Click OK to close the Add or Remove Snap-ins dialog box.
8. In the navigation tree, expand Certificates - Current User, expand Personal, and click Certificates.
9. In the Details pane, right-click the vpn1.satie.com certificate, click All Tasks, and click Export.
10. On the Welcome page, click Next.
11. On the Export Private Key page, click Yes, export the private key, and click Next.
12. On the Export File Format page, click Next to accept the default file format.
13. On the Password page, type **`Pass@word1`** in both text boxes, and click Next.
14. On the File to Export page, click Browse.
15. Under Favorites, click Desktop.
16. In the File name text box, type **`vpn1cert`** and click Save to save the certificate to the desktop.
17. Back on the File to Export page, click Next.
18. On the Completing the Certificate Export Wizard page, click Finish to close the wizard, and click OK in the confirmation dialog box.
19. In the console tree pane, expand Certificates (Local Computer), and expand Personal.
20. Right-click Certificates→All Tasks, and click Import.
21. On the Welcome page, click Next.
22. On the File to Import page, click Browse.
23. Under Favorites, click Desktop.
24. In the file type drop-down list, select Personal Information Exchange (*.pfx, *.p12).
25. In the list of files, double-click vpn1cert.
26. Back on the File to Import page, click Next.
27. On the Password page, type **`Pass@word1`** and click Next.
28. On the Certificate Store page, click Next to accept the Personal store location.
29. Click Finish to close the Import Export Wizard, and click OK in the confirmation dialog box.

Generating the trusted root certificate

1. On VPN1, in the Internet Explorer address bar, type `http://localhost/certsrv` and press Enter.
2. Under Select a task, click Download a CA certificate, certificate chain, or CRL.
3. Click Yes to allow the ActiveX control, and Yes to allow the certificate operation.
4. Click Download CA certificate.
5. Click Save, select Desktop, type the name `RootCACert`, click Save, and click Close. Later, you will move this certificate to the CLIENT1 computer.

Installing Network and Policy Access Server Role

1. On VPN1, in the Initial Configuration Tasks window, under Customize This Server, click Add roles.
2. On the Before You Begin page, click Next.
3. On the Select Server Roles page, click Network Policy and Access Services, click Next.
4. On the Network Policy and Access Services page, click Next.
5. On the Select Role Services page, select both Network Policy Server and Routing and Remote Access Services, and click Next.
6. On the Confirm Installation Selections page, click Install.
7. On the Installation Results page, click Close.
8. Now that the services are installed, you can configure them.

Configuring Routing and Remote Access

Configuring VPN1 to be a VPN server

1. On VPN1, click Start→Administrative Tools, and click Routing and Remote Access.
2. In the navigation tree, right-click VPN1 (local), and click Configure and Enable Routing and Remote Access.
3. On the Welcome to the Routing and Remote Access Server Setup Wizard page, click Next.
4. On the Configuration page, click Next to accept the default setting of Remote access (dial-up or VPN).
5. On the Remote Access page, select VPN, and click Next.
6. On the VPN Connection page, under Network interfaces, select Public. This is the interface that will connect VPN1 to the Internet.
7. Clear the option Enable security on the selected interface by setting up static packet filters, and click Next.
8. On the IP Address Assignment page, select From a specified range of addresses, and click Next.
9. On the Address Range Assignment page, click New.
10. On the New IPv4 Address Range dialog box, in Start IP address type `192.168.0.200`, in End IP address type `192.168.0.210`, click OK to add the range, and click Next. (This is the set of IP addresses available to assign to VPN clients).
11. On the Managing Multiple Remote Access Servers page, click Next to accept the default setting of not working with a RADIUS server. In this scenario, RRAS uses Windows Authentication.
12. On the Completing the Routing and Remote Access Server Setup Wizard page, click Finish.
13. On the warning about possible NPS policy conflicts, click OK.
14. On the warning about the need to configure the DHCP Relay Agent, click OK.

Configuring the Network Policy Server (NPS) to grant access for EAP-MSCHAPv2 authentication

Configuring the NPS server

1. Click Start→Administrative Tools, and click Routing and Remote Access.
2. On VPN1, in the Routing and Remote Access navigation tree, expand VPN1 (local).
3. Right-click Remote Access Logging & Policies, and then select Launch NPS.
4. In the Network Policy Server window, in the Network Access Policies section, click the Network Access Policies link.
5. Double-click Connections to Microsoft Routing and Remote Access server.

6. On the Overview tab, in the Access Permission section, select Grant access. Grant access if the connection request matches this policy.
7. On the Constraints tab, in the Contstraints list, select Authentication Methods.
8. If Microsoft: Secured password (EAP-MSCHAPv2) is not present in the EAP Types list, follow these steps:
    a. Click Add.
    b. In the Add EAP dialog box select Microsoft: Secured Password (EAP-MSCHAP v2), and click OK.
9. Select Microsoft: Smart Card or other certificate and click Remove to remove the EAP type.
10. Click OK to save your changes.
11. Close the Network Policy Server window.

Installing the operating system on the client (CLIENT1)

1. Insert the x64 Windows 7 Professional install DVD.
2. At the Install Windows screen, click Install Now.
3. At the Get Important updates for installation, click Go online to get the latest updates.
4. At the Select your operating system screen, select Windows 7 Professional, and click Next.
5. At the license agreement screen, check I accept the license terms, and click Next.
6. At the Which type of installation do you want screen, choose Upgrade, and click Next.
7. At the Help protect Windows Automatically, choose Ask me later.
8. Set the correct date and time, and click Next.
9. At the Thank you screen, click Start.
10. When the installer prompts you for a user name, type `User1`. When the installer prompts you for a computer name, type `CLIENT1`.
11. When the installer prompts you for a password, type a strong password twice.
12. When the installer prompts you for protection settings, click Use recommended settings.
13. When the installer prompts you for your computer's current location, click Work.
14. Connect CLIENT1 to a home network.

Installing Windows Updates on CLIENT1

We used Windows Update feature to install the following updates:

- Security Update for Microsoft .NET Framework 4 Client Profile (KB2446708)
- Security Update for Microsoft Windows (KB2425227)
- Security Update for Microsoft Windows (KB2446710)
- Security Update for Microsoft Windows (KB2479943)
- Security Update for Microsoft Windows (KB2491683)
- Security Update for Microsoft Windows (KB2497640)
- Security Update for Microsoft Windows (KB2503658)
- Security Update for Microsoft Windows (KB2506212)
- Security Update for Microsoft Windows (KB2506223)
- Security Update for Microsoft Windows (KB2507618)
- Security Update for Microsoft Windows (KB2508272)
- Security Update for Microsoft Windows (KB2508429)
- Security Update for Microsoft Windows (KB2509553)
- Security Update for Microsoft Windows (KB2510531)

- Security Update for Microsoft Windows (KB2511455)
- Security Update for Microsoft Windows (KB2524375)
- Update for Microsoft Windows (KB971033)
- Update for Microsoft Windows (KB976902)
- Update for Microsoft Windows (KB2484033)
- Update for Microsoft Windows (KB2488113)
- Update for Microsoft Windows (KB2502285)
- Update for Microsoft Windows (KB2505438)
- Update for Microsoft Windows (KB2511250)

Configuring TCP/IP

Configure TCP/IP properties so that CLIENT1 has a static IP address of 131.107.0.3 for the public (Internet) connection.

Configuring TCP/IP properties

1. On CLIENT1, click Start→Control Panel.
2. Under Network and Internet, click View network status and tasks.
3. In Network and Sharing Center, click Change adapter settings.
4. In Network Connections, right-click Local Area Connection, and click Properties.
5. In the Local Area Connection Properties dialog box, select Internet Protocol Version 4 (TCP/IPv4), and click Properties.
6. In the Intenet Protocol Version 4 (TCP/IPv4) Properties dialog box, click Use the following IP address. In IP address type `131.107.0.3` and in Subnet mask type `255.255.0.0`
7. Click OK, and click Close.

Configuring the hosts file

1. On CLIENT1, click Start→All Programs→Accessories, right-click Command Prompt, and click Run as administrator.
2. In the User Account Control dialog box, click Continue.
3. In the Administrator: Command Prompt window, type the following, and press Enter: `notepad %windir%\system32\drivers\etc\hosts`
4. Add the following text in a new line at the end of the document:

```
131.107.0.2          vpn1.satie.com
```

5. Save and close the hosts file.

Use Windows Firewall with Advanced Security to ensure that the appropriate firewall rules are enabled.

Ensuring that appropriate firewall rules in Windows Firewall with Advanced Security are enabled and configured to allow connections

1. On VPN1, click Start, type `wf.msc` and press Enter.
2. In the navigation tree, click Inbound Rules.
3. In the Details pane, double-click File and Printer Sharing (Echo Request - ICMPv4-In) for the Private and Public profiles.

4. In the Rule properties dialog box, under General select Enabled, under Action, select Allow the connection, and click OK.
5. Close the Windows Firewall with Advanced Security window.

Using ping to verify connection to vpn1.satie.com

1. On CLIENT1, in the Administrator: Command Prompt window, type `ping vpn1.satie.com` and press Enter.
2. Verify that you can successfully ping VPN1.
3. Close the Command Prompt window.

Configuring the VPN client with the root certificate

Installing the root certificate on the client

1. On CLIENT1, click Start, type `mmc` and press Enter.
2. In the Console1 window, click File, and click Add/Remove snap-in.
3. Under Available snap-ins, select Certificates, and click Add.
4. In the Certificates snap-in dialog box, select Computer account, and click Next.
5. In the Select Computer dialog box, click Finish to accept the default selection of Local computer.
6. Click OK to close the Add/Remove snap-ins dialog box.
7. In the navigation pane, expand Certificates (Local Computer), expand Trusted Root Certification Authorities, right-click Certificates, click All Tasks, and click Import
8. On the Certificate Import Wizard welcome page, click Next.
9. On the File to Import page, click Browse.
10. In the File name text box, type `\\vpn1.satie.com\c$\users\administrator.satie\desktop` and press Enter.
11. When asked for credentials, type `satie\administrator` and `Pass@word1`
12. Select RootCACert from the file list, and click Open.
13. With the path to certificate now complete, click Next.
14. On the Certificate Store page, click Next to select the default value of placing the certificate in the Trusted Root Certification Authorities store.
15. On the completion page, click Finish, and on the successful import notice, click OK.

Creating and configuring the remote connection with VPN reconnect on CLIENT1

Creating the VPN Reconnect connection to vpn1.satie.com

1. On CLIENT1, click Start→Control Panel.
2. Under Network and Internet, click View network status and tasks.
3. In Networking and Sharing Center, click Set up a new connection or network
4. Click Connect to a workplace, and click Next.
5. Click Use my Internet connection (VPN).
6. Click I'll set up an Internet connection later.
7. In Internet address, type `vpn1.satie.com`. In Destination name, type `VPN Reconnect Connection` and click Next.
8. In the Type your user name and password dialog box, type `user1` for the user name, and type `P@ssword1` for the password.
9. Click Remember this password.

10. In Domain, type `satie`
11. Click Create, and click Close.

Configuring and test the VPN Reconnect Connection

1. On CLIENT1, in Network and Sharing Center, click Change adapter settings.
2. Double-click VPN Reconnect Connection, and click Properties.
3. On the Security tab, in the Type of VPN list, select IKEv2, and click OK.
4. In the Connect VPN Reconnect Connection dialog box, click Connect.
5. If the Set Network Location dialog box appears, select Work.

CLIENT1 should successfully connect to VPN1 using the VPN Reconnect connection. To verify the connection, access the corporate file server from the CLIENT1 using the VPN Reconnect connection you just set up.

Testing the remote connection by connecting to a remote file share

1. Click Start→All Programs→Accessories →Run.
2. Type `\\dc1.satie.com\corpdata` and press Enter.
3. Double-click VPNTest to open it, add some text, and save the file.
4. Close Notepad.
5. In the Network Connections window, right-click VPN Reconnect Connection, and click Disconnect.

CONFIGURING THE NETWORK INFRASTRUCTURE FOR THE REMOTE MANAGEMENT TESTING

Configuring the domain controller

The domain controller is a server running Windows Server 2008 R2 Enterprise Edition. This server is configured as a domain controller with Active Directory and acts as the DNS and DHCP server for the intranet subnet. It also serves as an enterprise root CA for the domain.

Installing the operating system on the domain controller server and the ConfigMgr server

Install Windows Server 2008 R2 Enterprise Edition as a standalone server.

1. Start the installation of Windows Server 2008 R2.
2. Follow the instructions to complete the installation, specifying Windows Server 2008 R2 Enterprise Edition and a strong password for the local Administrator account. Log on using the local Administrator account.
3. Connect the network adapter to the Corpnet subnet.

Configuring TCP/IP on the domain controller server

Configure the TCP/IP protocol with a static IP address of 10.0.0.1 and the subnet mask of 255.255.255.0.

1. In Initial Configuration Tasks, click Configure networking.
2. In Network Connections, right-click Local Area Connection, and click Properties.
3. Click Internet Protocol Version 4 (TCP/IPv4), and click Properties.
4. Select Use the following IP address, type `10.0.0.1` next to IP address, and type `255.255.255.0` next to Subnet mask.
5. Click Advanced, and click the DNS tab.
6. In DNS suffix for this connection, type `corp.satie.com`, click OK twice, and click Close.

7. Close the Network Connections window.
8. In Initial Configuration Tasks, click Provide computer name and domain.
9. In System Properties, click Change. In Computer name, type `DC1`, click OK twice, and click Close. When the application prompts you to restart the computer, click Restart Now.
10. After restarting, log in using the local administrator account.
11. In Initial Configuration Tasks, click Do not show this window at logon, and click Close.

Configuring the server as a domain controller and DNS server

Configure the server as a domain controller and DNS server for the corp.satie.com domain.

1. In the console tree of Server Manager, click Roles. In the Details pane, click Add Roles, and click Next.
2. On the Select Server Roles page, click Active Directory Domain Services, click Add Required Features, click Next twice, and click Install. When installation is complete, click Close.
3. To start the Active Directory Installation Wizard, click Start, type `dcpromo` and press Enter.
4. In the Active Directory Installation Wizard dialog box, click Next twice.
5. On the Choose a Deployment Configuration page, click Create a new domain in a new forest, and click Next.
6. On the Name the Forest Root Domain page, type `corp.satie.com` and click Next.
7. On the Set Forest Functional Level page, in Forest Functional Level, click Windows Server 2008 R2, and click Next.
8. On the Additional Domain Controller Options page, click Next, click Yes to continue, and click Next.
9. On the Directory Services Restore Mode Administrator Password page, type a strong password twice, and click Next.
10. On the Summary page, click Next.
11. Wait while the wizard completes the configuration of Active Directory and DNS services, and click Finish.
12. When the application prompts you to restart the computer, click Restart Now.
13. After the computer restarts, log into the CORP domain using the Administrator account.

Installing and configuring DHCP

Configure DC1 as a DHCP server so that the test client can automatically configure itself when connecting to the Corpnet subnet.

1. In the console tree of Server Manager, click Roles.
2. In the Details pane, under Roles Summary, click Add roles, and click Next.
3. On the Select Server Roles page, click DHCP Server, and click Next twice.
4. On the Select Network Connection Bindings page, verify that 10.0.0.1 is selected, and click Next.
5. On the Specify IPv4 DNS Server Settings page, verify that corp.satie.com is listed under Parent domain.
6. Type `10.0.0.1` under Preferred DNS server IP address, and click Validate. Verify that the result returned is Valid, and click Next.
7. On the Specify WINS Server Settings page, accept the default setting of WINS is not required on this network, and click Next.
8. On the Add or Edit DHCP Scopes page, click Add.
9. In the Add Scope dialog box, type `Corpnet` next to Scope Name. Next to Starting IP Address, type `10.0.0.100` next to Ending IP Address, type `10.0.0.150` and next to Subnet Mask, type `255.255.255.0` Click OK, and click Next.

10. On the Configure DHCPv6 Stateless Mode page, select Disable DHCPv6 stateless mode for this server, and click Next.
11. On the Authorize DHCP Server page, select Use current credentials. Verify that CORP\Administrator is displayed next to User Name, and click Next.
12. On the Confirm Installation Selections page, click Install.
13. Verify the installation was successful, and click Close.

Installing an enterprise root CA on DC1

In this step, install an enterprise root CA on DC1 to provide computer certificates for domain member computers.

1. In the console tree of Server Manager, click Roles.
2. Under Roles Summary, click Add roles, and click Next.
3. On the Select Server Roles page, click Active Directory Certificate Services, and click Next twice.
4. On the Role Services page, click Next.
5. On the Setup Type page, click Enterprise, and click Next.
6. On the CA Type page, click Root CA, and click Next.
7. On the Private Key page, click Create a new private key, and click Next.
8. On the Cryptography page, click Next.
9. On the CA Name page, click Next.
10. On the Validity Period page, click Next.
11. On the Certificate Database page, click Next.
12. On the Confirm Installation Selections page, click Install.
13. On the Results page, click Close.

Installing and configuring IIS on the ConfigMgr server

1. On the ConfigMgr server, navigate to Start→All Programs→Administrative Tools→Server Manager to start Server Manager.
2. At the Select Features page of the Add Features Wizard, select BITS Server Extensions.
3. When the application prompts you to do so, click Add Required Role Services to add the dependent components, including the Web Server (IIS) role.
4. Select Remote Differential Compression, and click Next.
5. At the Web Server (IIS) page of the Add Features Wizard, click Next.
6. At the Select Role Services page of the Add Features Wizard, under Commen HTTP features, select WebDAV Publishing.
7. Under Application Development, select ASP.NET and, when the application prompts you to do so, click Add Required Role Services to add the dependent components.
8. Under Security, select Windows Authentication.
9. In the Management Tools node, under IIS 6 Management Compatibility, ensure that both IIS 6 Metabase Compatibility and IIS 6 WMI Compatibility are selected, and click Next.
10. At the Confirmation page, click Install, and complete the rest of the wizard.
11. Click Close to exit the Add Features Wizard, and close Server Manager.

Configuring WebDAV on the ConfigMgr server

1. Enable WebDAV, and create an Authoring Rule:
    a. Navigate to Start→All Programs→Administrative Tools→Internet Information Services (IIS) Manager to start Internet Information Services 7 Application Server Manager.

b. In the Connections pane, expand the Sites node in the navigation tree, and click Default Web Site if you are using the default Web site for the site system or SMSWEB if you are using a custom Web site for the site system.
c. In the Features View, double-click WebDAV Authoring Rules.
d. When the WebDAV Authoring Rules page appears, in the Actions pane, click Enable WebDAV.
e. After WebDAV has been enabled, in the Actions pane, click Add Authoring Rule.
f. In the Add Authoring Rule dialog box, under Allow access to, click All content.
g. Under Allow access to this content to, click All users.
h. Under Permissions, click Read, and click OK.

2. Change the property behavior:
   i. In the WebDAV Authoring Rules page, in the Actions pane, click WebDAV Settings.
   j. In the WebDAV Settings page, under Property Behavior, set Allow anonymous property queries to True.
   k. Set Allow Custom Properties to False.
   l. Set Allow property queries with infinite depth to True.
   m. If this is a BITS-enabled distribution point, under WebDAV Behavior, set Allow hidden files to be listed to True.
   n. In the Action pane, click Apply.
   o. Close Internet Information Services (IIS) Manager.

Joining the Active Directory Domain on the ConfigMgr server (both Dell and HP)

1. On the ConfigMgr server, click Start→Control Panel.
2. Double-click Network and Sharing Center.
3. Click Manage network connections.
4. Right-click the relevant connection, and select Properties.
5. Click Internet Protocol Version 4 (TCP/IPv4), and click Properties.
6. Click Use the following IP address, and enter a valid IP address for the domain.
7. Enter a valid subnet mask.
8. Click Use the following DNS server addresses, and enter the domain controller IP address.
9. Click OK, and click Close.
10. Close the Network Connections window.
11. Click Start→Control Panel.
12. Double-click System.
13. Click Change Settings.
14. Click Change.
15. Click Member of Domain.
16. Type the domain name, and click OK.
17. Enter the username and password of the domain administrator, and click OK.
18. Click OK on the Welcome to the domain dialog box.
19. Click OK twice.
20. Reboot the computer.
21. Shut down the ConfigMgr Server.

Creating Windows Security Groups for the Site System Servers

Use the following procedure to create Windows security groups for the site system servers. These security groups will be used to help ensure that only the required servers can use the two certificate templates required for AMT provisioning.

1. On the domain controller, click Start→Administrative Tools, and click Active Directory Users and Computers.
2. Right-click the domain, click New, and click Group.
3. In the New Object – Group dialog box, enter ConfigMgr Primary Site Servers as the Group name, and then click OK.
4. In Directory Users and Computers, right-click the group you have just created, and click Properties.
5. Click the Members tab, and click Add to select the member server.
6. Click OK, and click OK again to close the group properties dialog box.
7. Restart the ConfigMgr server.

Creating an Active Directory Organizational Unit

ConfigMgr requires an Active Directory container to store provisioned Intel AMT systems.

1. On the domain controller, click Start→Administrative Tools→Active Directory Users and Computers.
2. Right-click the domain name, and click New→Organizational Unit.
3. For the New Object name, type `Out of Band Management Controllers` and click OK.
4. Right-click Out of Band Management Controllers, and click Properties.
5. Select the Security tab, and click Add.
6. In the Enter the object names to select field, type ConfigMgr Primary Site Servers, and click OK.
7. Click ConfigMgr Primary Site Servers, and select Allow Full Control.
8. Click Advanced.
9. Select ConfigMgr Primary Site Servers, and click Edit.
10. In the Apply to drop down menu, select This object and all descendant objects.
11. Click OK on all three open properties windows, and close Active Directory Users and Computers.

Installing Windows Server Updates Services 3.0 SP2 on the ConfigMgr server (both Dell and HP)

1. Click Start→All Programs→Administrative Tools→Server Manager to start Server Manager.
2. Click Add Roles in the right pane of the Server Manager, and click Next.
3. At the Select Roles page, select Windows Server Update Services.
4. When the application prompts you to do so, click Add Required Role Services to add the dependent components, and click Next.
5. At the Introduction to Web Server (IIS) page, click Next.
6. At the Select Role Services page, click Next.
7. At the Windows Server Updates Services page, click Next.
8. At the Confirm Installation Selections page, click Install.
9. When the WSUS 3.0 SP2 setup Wizard starts, click Next.
10. At the License Agreement screen, click the I accept radio button, and click Next.
11. If you see a warning about a required component, click Next.
12. At the Select Update Source page, click Next.
13. At the Database Options page, click Next.
14. At the Web Site Selection page, click Next.
15. At the Ready to Install page, click Next.

16. At the Completing the Windows Server Update services screen, click Finish.
17. At the Before you Begin screen, click Next.
18. At the Microsoft Update Improvement Program, uncheck the Yes box, and click Next.
19. At the Choose Upstream Server screen, click Next.
20. At the Specify Proxy Server, click Next.
21. At the Connect to Upstream Server screen, select Start Connecting.
22. Skip to the next page in the wizard, and complete the steps in the wizard that begin on the To Continue installing WSUS 3.0 SP2 page.

Installing SQL Server 2008 R2 on the ConfigMgr server

1. Insert a SQL Server 2008 R2 Enterprise Edition DVD into the DVD drive.
2. If an AutoPlay window appears, click Run SETUP.EXE.
3. If an AutoPlay window does not appear, navigate to the DVD drive, and double-click to run SETUP.EXE.
4. At the Program Compatibility Assistant prompt, click Run program.
5. Click OK to install any remaining prerequisites SQL Server 2008 R2 requires.
6. When the SQL Server Installation Center window appears, click Installation.
7. Click New SQL Server stand-alone installation.
8. Click Run program.
9. After the Rule check completes with no errors, click OK.
10. Enter the product key for your copy of SQL Server 2008 R2, and click Next.
11. Check the box beside I accept the license terms, and click Next.
12. Click Install to install Setup Support Files.
13. Once the Setup Support Files finish installing, SQL Server 2008R2 Setup will open a new window.
14. SQL Server 2008 will then run a check of the Setup Support Rules.
15. Once it is finished with no errors, click Next.
16. At the Feature Selection screen, check the box beside the following features:
    - Database Engine Services
    - Reporting Services
    - Client Tools Connectivity
    - Client Tools Backwards Compatibility
    - Management Tools – Basic
    - Management Tools – Complete
17. Click Next.
18. At the Instance Configuration screen, accept the defaults, and click Next.
19. Ensure that you have the required disk space to install, and click Next.
20. Enter domain credentials for SQL Server service account, and click Next.
21. Keep Windows Authentication selected, and click Add Current User.
22. Click Next.
23. At the Error and Usage Reporting screen, click Next.
24. Once the Installation Rules check is complete, click Next.
25. Click Install.
26. When the Installation is complete, click Next.
27. Click Close.
28. Close all windows.

Extending the Active Directory schema for ConfigMgr[1] on the domain controller server

1. Extend the Active Directory schema:
    a. On the Active Directory machine, log in with domain administrator privileges.
    b. Disconnect the domain controller from the network by unplugging the network cable.
    c. Extract the ConfigMgr installation to the Active Directory server.
    d. At a command prompt, browse to the C:\SCConfigMgr07_EVAL_EN \SMSSETUP\BIN\I386 folder.
    e. Run extadsch.exe, located in the C:\SCConfigMgr07_EVAL_EN \SMSSETUP\BIN\I386 folder on the Configuration Manager 2007 installation media, to add the new classes and attributes to the Active Directory schema.
    f. Verify that the schema extension was successful by reviewing the extadsch.log, located in the root of the system drive.
    g. Reconnect the domain controller to the network.
2. Create the System Management container:
    a. On the Active Directory machine, on the taskbar, click Start, and click Run.
    b. Type `adsiedit.msc` and click OK.
    c. Right-click ADSI Edit, and connect to the domain in which the site server resides.
    d. In the console pane, expand Domain, expand hpmelville, and right-click CN=System.
    e. Click New, and click Object.
    f. In the Create Object dialog box, select Container, and click Next.
    g. In the Value field, type System Management, and click Next.
    h. Click Finish.
3. Set security permissions on the System Management container:
    a. On the Active Directory machine, on the taskbar, click Start, and click Run.
    b. Type `adsiedit.msc` and click OK.
    c. Right-click ADSI Edit, and connect to the domain in which the site server resides.
    d. In the console pane, expand Domain, expand dellmelville, and expand CN=System.
    e. Right-click CN=System Management, and select Properties.
    f. Click the Security tab.
    g. Click Add to add the site server computer account, and grant Full Control permissions.
    h. Click Advanced, select the site server's computer account, and click Edit.
    i. In the Apply onto list, select This object and all descendant objects, and click OK.
    j. Click OK twice.
    k. Restart the Active Directory Machine.

Running the prerequisite checker for System Center Configuration Manager 2007 SP2 on the ConfigMgr server

1. Insert the System Center Configuration Manager 2007 SP2 installation disk.
2. When the Auto-run screen appears, select splash.hta.
3. At the Start screen, click Run the prerequisite checker.

[1] Source: http://technet.microsoft.com/en-us/library/bb633121.aspx

4. At the Installation Prerequisite Check Options screen, click the Primary Site radio button, and enter the machine name for SQL Server and machine name for SDK Server. Click OK.
5. At the Installation Prerequisite Check, no further prerequisites should be required.
6. Close the prerequisite checker.

Installing Microsoft System Center Configuration Manager 2007 SP2 on the ConfigMgr server

1. Insert the System Center Configuration Manager 2007 SP2 installation disk.
2. When the Auto-run screen appears, select splash.hta.
3. Under Install, click Configuration Manager 2007 SP2.
4. At the Welcome screen, click Next.
5. At the Available Setup Options screen, click the Install a Configuration Manager site server radio button, and click Next.
6. At the Microsoft Software License Terms screen, check the I accept these license terms checkbox, and click Next.
7. At the Installation Settings screen, click the Custom settings radio button, and click Next.
8. At the Site Type screen, click the Primary site radio button, and click Next.
9. At the Customer Experience Improvement Program Configuration screen, click the No, I do not want to participate right now radio button, and click Next.
10. At the Product Key screen, enter the product key, and click Next.
11. At the Destination Folder screen, click Next.
12. At the Site Settings screen, create a Site code and Site name, type them in the appropriate text boxes, and click Next.
13. At the Site Mode screen, click the Configuration Manager Mixed Mode radio button, and click Next.
14. At the Client Agent Selection screen, click Next.
15. At the Database Server screen, enter the SQL Server and instance and ConfigMgr site database information, and click Next.
16. At the SMS Provider Settings screen, enter the installation location for the provider, and click Next.
17. At the Management point screen, click the install a management point radio button, and click Next.
18. At the Port Settings screen, ensure that the Use default port (80) radio button is selected, and click Next.
19. At the Updated Prerequisite Components screen, click Check for updates and download newer versions to an alternate path radio, and click Next.
20. At the Updated Prerequisite Component Path screen, specify the alternate path for storage of updated components, and click Next.
21. At the Success screen, click Begin Install.
22. At the Settings Summary screen, review the settings, and click Next.
23. At the Setup Action Status Monitoring screen, click Begin Install.
24. When installation completes, click Next.
25. At the Completing the Microsoft System Center Configuration Manager 2007 SP1 Setup Wizard screen, click Finish.

Patching Microsoft System Center Configuration Manager 2007 SP2 to R3

1. Before patching to Microsoft System Center Configuration Manager 2007 R3, download and install the prerequisite hotfix KB977384: http://support.microsoft.com/kb/977384.

2. Download the Microsoft System Center Configuration Manager 2007 R3 patch from http://technet.microsoft.com/en-us/evalcenter/bb736730.aspx.
3. Run the executable, and click Install Configuration Manager 2007 R3.
4. Finish the install by accepting all defaults.

Installing the Out of Band Service Point role in ConfigMgr

1. Open the Configuration Manager console.
2. On the left-hand side, navigate to Site Database→Site Management→Site Code→Site Settings→Site Systems.
3. Right-click the ConfigMgr server, and click New Roles.
4. On the General page, click Next.
5. On the Site Role Selection page, select Out of band service point, and click Next.
6. On the Out of Band Service Point page, accept all the defaults, and click Next.
7. Click Next on the summary page, and click Close when the installation is complete.

Creating the AMT Provisioning and Web Server Certificates

1. On the domain controller, click Start→Administrative Tools→Certification Authority.
2. Expand the server name, right-click Certificate Templates, and click Manage.
3. In the Template Display Name column, right-click Web Server, and click Duplicate Template.
4. Select Windows Server 2003 Enterprise Edition, and click OK.
5. On the General tab, enter `ConfigMgr AMT Provisioning` for the AMT provisioning certificate name.
6. On the Request Handling tab, select Allow private key to be exported.
7. On the Subject Name tab, select Build from this Active Directory information, and select Common name.
8. On the Extensions tab, select Application Policies, and click Edit.
9. Click Add.
10. Click New.
11. Type `AMT Provisioning` in the Name field, and type `2.16.840.1.113741.1.2.3` for the Object identifier.
12. Click OK.
13. Click OK to close the Add Application Policy dialog box.
14. Click OK to close the Edit Application Policies Extension dialog box.
15. Ensure that Server Authentication and AMT Provisioning are listed in the Application Policies description.
16. On the Security tab, remove the Enroll permission from Domain Admins and Enterprise Admins.
17. Click Add, and enter ConfigMgr Primary Site Servers in the text box.
18. Click OK.
19. Click ConfigMgr Primary Site Servers, and select Allow Read and Enroll.
20. Click OK, and close the Certificate Templates window.
21. In the Certification Authority console, right-click Certificate Templates.
22. Click New→Certificate Template to Issue.
23. Select ConfigMgr AMT Provisioning, and click OK.
24. Right-click Certificate Templates, and click Manage.
25. In the Template Display Name column, right-click Web Server, and click Duplicate Template.

26. Select Windows Server 2003 Enterprise Edition, and click OK.
27. On the General tab, enter `ConfigMgr AMT Web Server Certificate` for the certificate name.
28. On the Security tab, remove the Enroll permission from Domain Admins and Enterprise Admins.
29. Click Add, and enter `ConfigMgr Primary Site Servers` in the text box.
30. Click OK.
31. Click Publish to Active Directory.
32. Click ConfigMgr Primary Site Servers, and select Allow Read, Enroll, and Auto-enroll.
33. On the Security Tab, Click Add.
34. Click Object Types and select Computers.
35. In the Object Name type ConfigMgr Primary Site Servers and Check Name.
36. Under Permissions check Allow Read and Enroll.
37. Click OK, and close the Certificate Templates window.
38. In the Certification Authority console, right-click Certificate Templates.
39. Click New→Certificate Template to Issue.
40. Select ConfigMgr AMT Web Server Certificate, and click OK.
41. Close Certification Authority.

Installing and exporting the AMT provisioning certificate on the ConfigMgr server

1. On the ConfigMgr server, click Start→Run.
2. Type `mmc.exe` and press Enter.
3. When the console appears, click File→Add/Remove Snap-in.
4. Select Certificates, and click Add.
5. Select Computer account, and click Next.
6. Ensure Local computer: (the computer this console is running on) is selected, and click Finish.
7. Click OK.
8. In the console, expand Certificates (Local Computer).
9. Right-click Personal, and click All Tasks→Request New Certificate.
10. Click Next.
11. Click Next.
12. Select ConfigMgr AMT Provisioning, and click Enroll.
13. Click Finish.
14. Open Personal→Certificates.
15. Right-click ConfigMgr AMT Provisioning, and click All Tasks→Export.
16. Click Next.
17. Select Yes, export the private key, and click Next.
18. Select Personal Information Exchange - PKCS #12 (.PFX), and select Include all certificates in the certificate path if possible.
19. Enter a password, and click Next.
20. Browse to the C:\ drive, and enter a name for the exported certificate.
21. Click Next.
22. Click Finish.
23. Click OK in the Certificate Export Wizard dialog box.

Configuring the Out of Band Management Service Point

1. On the ConfigMgr server, open the Configuration Manager Console for System Center.
2. On the left-hand side, navigate to Site Database→Site Management→Site Code→Site Settings→Component Configuration.
3. Right-click Out of Band Management, and click Properties.
4. On the General tab, click Browse for the Active Directory container.
5. Select Out of Band Management Controllers, and click OK.
6. Click Set for the MEBx Account.
7. Enter the password that will be changed from the default password for the admin MEBx account, and click OK.
8. Select Allow out of band provisioning.
9. At the security warning, click Yes.
10. Leave the default port of 9971.
11. Select Register ProvisionServer as an alias in DNS.
12. Click Browse for the Provisioning Certificate.
13. Click Browse.
14. Navigate to the exported certificate from the previous section.
15. Select the certificate, and click Open.
16. Enter the password for the certificate, and click OK.
17. Click Select for the Certificate template.
18. Under AMT certificate template, select ConfigMgr AMT Web Server Certificate, and click OK.
19. Click Apply.
20. On the AMT Settings tab, click the star button to add a new AMT user account.
21. Add the domain administrator account, and select Platform Administration.
22. Click OK.
23. Select a default IDE-redirect image if applicable.
24. Leave the default power state.
25. Check the following boxes:
    - Enable Web interface for AMT systems
    - Enable serial over LAN and IDE-redirect for AMT systems
    - Allow ping responses
    - Enable BIOS password bypass for power on and restart commands
    - Enable support for Intel WS-MAN Translator
26. Leave the default setting of 5 for the Kerberos clock tolerance level.
27. Click Apply.
28. On the Provisioning Settings tab, click the star button to add a new AMT provisioning and discovery account.
29. Enter the user name and password for the MEBx account set on target AMT systems.
30. Click OK.
31. Click OK to finish configuring the Out of Band service point.

Configuring Network Discovery for AMT Controllers

1. On the left-hand side, navigate to Site Database→Site Management→Site Code→Site Settings→Discovery Methods.

2. Right-click Network Discovery, and click Properties.
3. On the General tab, check the box for Enable discovery of out of band management controllers.
4. Click OK.

Configuring a New Site Boundary

1. On the left-hand side, navigate to Site Database→Site Management→Site Code→Site Settings.
2. Right-click Boundaries, and click New Boundary.
3. In the Description field, type a name for the new boundary.
4. For the Type, select IP address range from the dropdown menu.
5. Enter a starting IP address and an ending IP address appropriate to the test bed network.
6. Click OK.

Creating and Configuring a New Collection for Unprovisioned vPro Clients

1. On the left-hand side, navigate to Site Database→Computer Management→Collections.
2. Right-click collections, and click New collection.
3. In the Name field, type `Unprovisioned vPro Clients`
4. Click Next.
5. Click the Query Rule Properties button represented by a database icon.
6. In the Query Rule Properties window, click Edit Query Statement.
7. Click Show Query Language.
8. In the Query Statement textbox type `Select * from SMS_R_System where AMTStatus=2`
9. Click OK.
10. On the Query Rule Properties window, click OK.
11. In the Membership Rules window, click Next.
12. On the Advertisements page, click Next.
13. On the Security page, accept the defaults, and click Next.
14. Click Close.
15. Under Collections, right-click the new collection Unprovisioned vPro Clients.
16. Click Modify Collection Settings.
17. Select the Out of Band tab, and check the box for Enable automatic out of band management controller provisioning.
18. Click OK.
19. Add the columns for AMT Status, AMT Version, and Automatic AMT Provisioning to both the Unprovisioned vPro Clients collection and the All Systems Collection.

Adding the AMT Provisioning Certificate Hash to the List of Active Hashes in Intel AMT on target AMT systems

Before running a system discovery in the ConfigMgr console, the target AMT controllers need to be configured with the CA hash hosting the AMT Provisioning certificate created in a previous step. If a third-party certificate was used, Intel AMT is preconfigured with active hashes from popular domain providers such as GoDaddy.com® and VeriSign®.

1. On the domain controller, click Start→Run…
2. Type `mmc.exe` and press Enter.
3. When the console appears, click File→Add/Remove Snap-in.
4. Select Certificates, and click Add.
5. Select Computer account, and click Next.

6. Ensure Local computer: (the computer this console is running on) is selected, and click Finish.
7. Click OK.
8. In the console, navigate to Certificates (Local Computer)→Personal→Certificates.
9. Double-click the certificate in the center pane named corp-DC1-CA.
10. In the Certificate properties window, click the Details pane.
11. Scroll down to the bottom of the list, and select Thumbprint.
12. Write down the 20 byte hexadecimal certificate hash.
13. Close all windows.
14. On the target AMT System, login to the Intel MEBx BIOS.
15. Change the password to match the AMT administrator account specified in the steps for Configuring the Out of Band Management Point.
16. Select Intel AMT Configuration→Setup and Configruation→TLS PKI→Manage Certificate Hashes.
17. Press Insert to create a new certificate hash entry.
18. Enter a new name for the certificate hash, and press Enter.
19. Enter the 20 byte hexadecimal certificate hash written down from domain controller thumbprint.
20. Press Enter.
21. Press `Y` to set the certificate as active.
22. Exit the MEBx BIOS, saving all changes.
23. Before returning to the ConfigMgr server, ensure the target system's operating system is logged into the domain and the firewall is disabled.

Configuring Active Directory System Discovery

1. On the ConfigMgr server, open the ConfigMgr Console.
2. On the left-hand side, navigate to Site Database→Site Management→Site Code→Site Settings→Discovery Methods.
3. Right-click Active Directory System Discovery, and click Properties.
4. On the General tab, click the star button to add a new Active Directory container for discovery.
5. Select Local Domain, and click OK.
6. Select the Computers container, and click OK.
7. On the Polling Schedule tab, check the box for Run discovery as soon as possible, and click OK.
8. On the left-hand side, navigate to Site Database→Computer Management→Collections.
9. Right-click Collections, and click Update Collection Membership.
10. Click Yes to confirm.
11. Select the All Systems collection, and refresh until the target system's computer name appears in the list. The update can take several minutes to complete.
12. Under the AMT status column, the target system should be listed as Unknown.
13. Right-click the target system, and click Out of Band Management→Discover Management Controllers.
14. Click OK to initiate the discovery.
15. Right-click Collections, and select Update Collection Membership.
16. Click Yes to confirm.
17. Select the Unprovisioned vPro Clients collection, and refresh until the target system appears. This update can take several minutes to complete.
18. Under the AMT status column, the target system should now be listed as Not Provisioned.

Configuring the target AMT system with the Configuration Manager Client

To start the automatic provisioning process, the target AMT system must be configured with the Configuration Manager Client.

1. On the ConfigMgr server, navigate to C:\Program Files (x86)\Microsoft Configuration Manager.
2. Copy the Client folder to a USB drive.
3. Copy the Client folder to the C:\ drive of the tartget AMT system.
4. On the target AMT system, login to the domain as the domain administrator account.
5. Open a command prompt, and navigate to C:\Client.
6. Run the following command: `ccmsetup.exe /mp:SCCMServerName /logon smssitecode=3LetterSCCMSiteCode`
7. Open Task Manager, and click the Processes tab.
8. Once the installation is complete, the CcmExec.exe process will be running.
9. Open Control Panel, and select Classic view.
10. Double-click Configuration Manager.
11. Click the Actions tab.
12. Select Machine Policy Retrieval & Evaluation Cycle, and click Initiate Action.
13. Click OK.
14. Select User Policy Retrieval & Evaluation Cycle, and click Initiate Action.
15. Click OK.
16. Click OK to close the Configuration Manager Properties window.
17. Wait a few minutes, double-click on the Configuration Manager icon in the Control Panel.
18. On the Actions tab, there should now be a longer list of actions to initiate.
19. Close the Configuration Manager Properties window.

Updating the ConfigMgr collections to discover provisioned AMT controllers

1. On the ConfigMgr server, open the Configuration Manager Console.
2. On the left-hand side, navigate to Site Database→Computer Management→Collections.
3. Right-click Collections, and click Update Collection Membership.
4. Click Yes to confirm.
5. Select the Unprovisioned vPro Clients collection, and refresh until the target AMT system disappears from the collection. The update can take several minutes to complete.
6. Select the All Systems collection. The target AMT system should now have an AMT status of Provisioned.

Installing Intel vPro Technology Activator Utility

For the next steps you will need to download Intel's Activator Utility. You can find it at http://software.intel.com/en-us/articles/intel-vpro-technology-activator-utility/.

1. On the Client, copy the Intel vPro Activator to the root of C:
2. Open command prompt.
3. Navigate to the folder containing the activator.
4. Type `activator.exe /s http://localhost/ /c /h`
5. On the ConfigMgr server, open the Configuration Manager Console.
6. On the left-hand side, navigate to Site Database→Computer Management→Collections→All Systems.
7. In the middle Pane, right-click and select Refresh until your AMT Provisioning Status changes to Provisioned. Measuring battery life with BAPCo MobileMark 2007 v.1.06

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.