Statement of Volatility – Dell EMC PowerEdge T440

Dell EMC PowerEdge T440 contains both volatile and non-volatile (NV) components. Volatile components lose their data immediately upon removal of power from the component. Non-volatile components continue to retain their data even after the power has been removed from the component. Components chosen as user-definable configuration options (those not soldered to the motherboard) are not included in the Statement of Volatility. Configuration option information (pertinent to options such as microprocessors, remote access controllers, and storage controllers) is available by component separately. The following NV components are present in the PowerEdge T440 server.

Item	Non-Volatile or Volatile	Quantity	Reference Designator	Size
Planer				
PCH Internal CMOS RAM	Non-Volatile	1	U_PCH1	256 Bytes
BIOS SPI Flash	Non-Volatile	1	U_PRIM_SPI_BIOS	32 MB
BIOS Recovery SPI Flash	Non-Volatile	1	U_RECROM	16 MB
iDRAC SPI Flash	Non-Volatile	1	U_UBOOT	4 MB
BMC EMMC	Non-Volatile	1	U_EMMC1	8 GB
System CPLD RAM	Volatile	1	U_CPLD1	16 KB
System Memory	Volatile	Up to 10 for CPU1 Up to 6 for CPU2	CPU1: A1~A10, CPU2: B1~B6	Up to 32GB per DIMM (RDIMM) Up to 64GB per DIMM (LRDIMM)
Internal USB Key	Non-Volatile	1	J_USB3_INT	Varies (not factory installed)
Trusted Platform Module (TPM, TPM 2.0 only)	Non-Volatile	1	J_TPM_MODULE	128 Bytes
CPU Vcore and VSA Regulators	Non-Volatile	1 for CPU1, 1 for CPU2	PAAU1 PBAU1	16KB
Memory VDDQ Regulators	Non-Volatile	2 for CPU1, 2 for CPU2	PAEU2, PAFU2 PBEU2, PBFU2	16KB
LOM NVRAM	Non-Volatile	1	U_LOM1_ROM	1 MB
Power Supplies				
Microcontroller	Non-Volatile	Up to 2	Microchip	Up to 64KB

Item	Non-Volatile or Volatile	Quantity	Reference Designator	Size
5U 8x3.5” Backplane				
SEP internal flash	Non-Volatile	1	U_SEP	Flash:64KB+4KB EEPROM:2KB SRAM: 4KB
5U 16x2.5” EXP/Backplane				
SAS Expander flash	Non-Volatile	1	U_EXP_FLASH	128Mbit
BP FRU image	Non-Volatile	1	U_BP_FRU	EEPROM:4KB
Expander FRU image	Non-Volatile	1	U_EXP_FRU	EEPROM:4KB
H740, H740P, H840 PERC				
NVSRAM memory	Non-Volatile	1	U1087	128KB
FRU	Non-Volatile	1	U1019	256B
SPD	Non-Volatile	1	U22	256B
Flash	Non-Volatile	1	U1086	16MB
Backup Flash	Non-Volatile	1	U1100	8GB
SDRAM	Volatile	9	U1077-U1085	8GB
H330 PERC				
NVSRAM memory	Non-Volatile	1	U1033	128KB
FRU	Non-Volatile	1	U1019	256B
1-Wire EEPROM	Non-Volatile	1	U1004	128B
SBR	Non-Volatile	1	U1020	8KB
Flash	Non-Volatile	1	U3	16MB
HBA 330 PERC				
NVSRAM memory	Non-Volatile	1	U1033	128KB
FRU	Non-Volatile	1	U1019	256B
Serial Boot ROM	Non-Volatile	1	U1020	8KB
Flash	Non-Volatile	1	U3	16MB
TPM				
Trusted Platform Module (TPM, TPM 2.0 only)	Non-Volatile	1	U_TPM	128 Bytes
IDSDM - vFlash				

Dell - Internal Use - Confidential

Item	Non-Volatile or Volatile	Quantity	Reference Designator	Size
vFlash (uSD)	Non-Volatile	1	J3	16GB
iDSDM (uSD1, uSD2)	Non-Volatile	2	J1, J2	16GB, 32GB, 64GB
SPI Flash	Non-Volatile	1	U2	1MB
BOSS				
SPI Flash	Non-Volatile	1	U17	1024KB
TFRU	Non-Volatile	1	U7	64KB

Dell - Internal Use - Confidential

Item	Type (e.g. Flash PROM, EEPROM)	Can user programs or operating system write data to it during normal operation?	Purpose? (e.g. boot code)
Planer			
PCH Internal CMOS RAM	Battery-backed CMOS RAM	No	Real-time clock and BIOS configuration settings
BIOS SPI Flash	SPI Flash	Yes	Boot code, system configuration information, UEFI environment, Flash Disceptor, ME
BIOS Recovery SPI Flash	SPI Flash	No	16MB Recovery SPI ROM exits as an aid to reprogram the primary ROM
iDRAC SPI Flash	SPI Flash	No	iDRAC Uboot (bootloader), server managent persistent store (i.e. IDRAC MAC Address, iDRAC boot variables), lifecycle log cache, virtual planar FRU and EPPID, rac log, System Event Log,
BMC EMMC	eMMC NAND Flash	No	Operational iDRAC FW, Lifecycle Controller (LC) USC partition, LC service diags, LC OS drivers, USC firmware
Memory VDDQ, CPU Vcore and VSA Regulators	OTP(one time programmable)	No	Operational parameters
System CPLD RAM	RAM	No	Not utilized
System Memory	RAM	Yes	System OS RAM
Internal USB Key	Flash	Yes	General purpose USB key drive
Trusted Platform Module (TPM, TPM 2.0 only)	EEPROM	Yes	Storage of encryption keys
Power Supplies			
Microcontroller	Flash PROM and EEPROM	Yes	Report PSU information and control firmware

Dell - Internal Use - Confidential

Item	Type (e.g. Flash PROM, EEPROM)	Can user programs or operating system write data to it during normal operation?	Purpose? (e.g. boot code)
5U 8x3.5" Backplane			
SEP internal flash	Flash	No	FW configuration data
SEP internal EEPROM	EEPROM	No	FRU
5U 16x2.5" EXP/Backplane			
Flash memory	Flash	No	Card firmware
BP FRU image	EEPROM	No	FRU
Expander FRU image	EEPROM	No	FRU
H740, H740P, H840 PERC			
NVSRAM memory	NVSRAM	No	Configuration data
FRU	FRU	No	Card manufacturing information
SPD	SPD	No	Memory configuration data
Flash	Flash	No	Card firmware
Backup Flash	Backup Flash	No	Holds cache data during power loss
SDRAM	SDRAM	No	Cache for HDD I/O
H330 PERC			
NVSRAM memory	NVSRAM	No	Configuration data
FRU	FRU	No	Card manufacturing information
1-Wire EEPROM	1-Wire EEPROM	No	Holds default controller properties/settings
SBR	SBR	No	Boot loader
Flash	Flash	No	Card firmware
HBA 330 PERC			
NVSRAM memory	NVSRAM	No	Configuration data
FRU	FRU	No	Card manufacturing information

Dell - Internal Use - Confidential

Item	Type (e.g. Flash PROM, EEPROM)	Can user programs or operating system write data to it during normal operation?	Purpose? (e.g. boot code)
Serial Boot ROM	Serial Boot ROM	No	Boot loader
Flash	Flash	No	Card firmware
TPM			
Trusted Platform Module (TPM, TPM 2.0 only)	EEPROM	Yes	Storage of encryption keys
IDSDM - vFlash			
vFlash (uSD)	NAND flash	Yes	Populate out-of-band or optionally connect to the host as mass storage and boot mechanism
iDSDM (uSD1, uSD2)	NAND flash	Yes	Provides mass storage
SPI Flash	SPI Flash	It is only indirectly connected to iDRAC. iDRAC can read any address in the SPI flash, but may only write the primary firmware storage area as a part of a firmware update procedure.	Boot firmware storage, configuration and state data for IDSDM.
BOSS			
SPI Flash	FLASH EEPROM	No	Boot code, FW
TFRU	FLASH EEPROM	Yes	Thermal monitoring

Dell - Internal Use - Confidential

Item	How is data input to this memory?	How is this memory write protected?	How is the memory cleared?
Planer			
PCH Internal CMOS RAM	BIOS	N/A – BIOS only control	1) Set NVRAM_CLR jumper to clear BIOS configuration settings at boot and reboot system. 2) Power off the system, remove coin cell battery for 30 seconds, replace battery and then power back on. 3) Restore default configuration in F2 system setup menu.
BIOS SPI Flash	SPI interface via iDRAC	Software write protected	Not possible with any utilities or applications and system is not functional if corrupted or removed.
BIOS Recovery SPI Flash	SPI interface via PCH	Software write protected	Not possible with any utilities or applications and the system is not functional if BIOS SPI is corrupted or removed.
iDRAC SPI Flash	SPI interface via iDRAC	Embedded iDRAC subsystem firmware actively controls sub area based write protection as needed.	The user cannot clear memory completely. However, user data, lifecycle log and archive, SEL, and fw image repository can be cleared using Delete Configuration and Retire System, which can be accessed through the Lifecycle Controller interface.
BMC EMMC	NAND Flash interface via iDRAC	Embedded FW write protected	The user cannot clear memory completely. However, user data, lifecycle log and archive, SEL, and fw image repository can be cleared using Delete Configuration and Retire System, which can be accessed through the Lifecycle Controller interface.
Memory VDDQ, CPU Vcore and VSA Regulators	Once values are loaded into register space a cmd writes to nvm.	There are passwords for different sections of the register space	The user cannot clear memory.

Dell - Internal Use - Confidential

Item	How is data input to this memory?	How is this memory write protected?	How is the memory cleared?
System CPLD RAM	Not utilized	Not accessible	Not accessible
System Memory	System OS	OS Control	Reboot or power down system
Internal USB Key	USB interface via PCH. Accessed via system OS	No write protect	Can be cleared in the system OS
Trusted Platform Module (TPM, TPM 2.0 only)	Using TPM Enabled operating systems	SW write protected	F2 Setup option
Power Supplies			
Microcontroller	The data is flash via Dell Update Package(DUP)	Using signature and manufacture key to protect memory write	Before firmware update, the memory will be clear.
5U 8x3.5" Backplane			
SEP internal flash	Pre-programmed before assembly	Not WP	The user cannot clear memory.
SEP internal EEPROM	Programmed at ICT during production.	Not WP	The user cannot clear memory.
5U 16x2.5" EXP/Backplane			
Flash memory	Pre-programmed before assembly. Can be updated using Dell/LSI tools	Not WP. Not visible to Host Processor	Cannot be cleared with existing tools available to the customer
BP FRU image	Programmed at ICT during production.	Not WP	The user cannot clear memory.
Expander FRU image	Programmed at ICT during production.	Not WP	The user cannot clear memory.
H740, H740P, H840 PERC			
NVSRAM memory	ROC writes configuration data to NVSRAM	Not WP. Not visible to Host Processor	User cannot clear the memory.
FRU	Programmed at ICT during production.	Not WP	User cannot clear the memory.
SPD	Pre-programmed before assembly	Not WP. Not visible to Host Processor	User cannot clear the memory.
Flash	Pre-programmed before assembly. Can be updated using Dell/LSI tools	Not WP. Not visible to Host Processor	User cannot clear the memory.
Backup Flash	FPGA backs up DDR data to this device in case of a power failure	Not WP. Not visible to Host Processor	Flash can be cleared by powering up the card and allowing the controller to flush the contents to VDs. If the VDs are no longer available, cache can be cleared by going into

Dell - Internal Use - Confidential

Item	How is data input to this memory?	How is this memory write protected?	How is the memory cleared?
			controller BIOS and selecting Discard Preserved Cache.
SDRAM	ROC writes to this memory - using it as cache for data IO to HDDs	Not WP. Not visible to Host Processor	Cache can be cleared by powering off the card
H330 PERC			
NVSRAM memory	ROC writes configuration data to NVSRAM	Not WP. Not visible to Host Processor	Cannot be cleared with existing tools available to the customer
FRU	Programmed at ICT during production.	Not WP	Cannot be cleared with existing tools available to the customer
1-Wire EEPROM	ROC writes data to this memory	Not WP. Not visible to Host Processor	Cannot be cleared with existing tools available to the customer
SBR	Pre-programmed before assembly	Not WP. Not visible to Host Processor	Cannot be cleared with existing tools available to the customer
Flash	Pre-programmed before assembly. Can be updated using Dell/LSI tools	Not WP. Not visible to Host Processor	Cannot be cleared with existing tools available to the customer
HBA 330 PERC			
NVSRAM memory	ROC writes configuration data to NVSRAM	No write protect. Not visible to Host Processor	The user cannot clear memory.
FRU	Programmed at ICT during production	No write protect	The user cannot clear memory.
Serial Boot ROM	Pre-programmed before assembly	No write protect. Not visible to Host Processor	The user cannot clear memory.
Flash	Pre-programmed before assembly. Can be updated using Dell/LSI tools	No write protect. Not visible to Host Processor	The user cannot clear memory.
TPM			
Trusted Platform Module (TPM, TPM 2.0 only)	Using TPM Enabled operating systems	SW write protected	F2 Setup option
IDSDM - vFlash			
vFlash (uSD)	User can provide data to iDRAC (entirely in the iDRAC domain) to be pushed into vFlash	No write protect	1. The card may be physically removed and destroyed or cleared via standard means on a separate computer. Or 2. The user has access to the card in the host domain and may clear it manually.
iDSDM (uSD1, uSD2)	Device resides in host domain; they are exposed to the user via an	Physical write protect switch on ACE card	(1) card may be physically removed and destroyed or cleared via standard

Dell - Internal Use - Confidential

Item	How is data input to this memory?	How is this memory write protected?	How is the memory cleared?
	internally connected, non-removable USB mass storage device		means on a separate computer OR (2)User has access to the card in the host domain and may clear it manually
SPI Flash	User can initiate a firmware update of the IDSDM device.	There is no mechanism provided to iDRAC to write any SPI NOR area outside of the primary IDSDM firmware region.	iDRAC may issue a clear command to erase all contents of the SPI NOR, but doing this will leave the IDSDM non-functional.
BOSS			
SPI Flash	By programming the image via firmware update process	N/A	Use Flash tool, type "go.nsh w y"
TFRU	During Manufacturing, by programming the image via firmware update process. During runtime, by I2C Proprietary Command Protocol	N/A	By writing to Flash

NOTE: For any information that you may need, direct your questions to your Dell Marketing contact.

Dell - Internal Use - Confidential