DELL Technologies

Statement of Volatility – Dell EMC PowerEdge T350

Dell EMC PowerEdge T350 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 T350 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	U6	32 MB
BIOS Data SPI Flash	Non-Volatile	1	U3	4 MB
iDRAC SPI Flash	Non-Volatile	1	U7	4 MB
BMC EMMC	Non-Volatile	1	U21	8 GB
iDRAC DDR4	Volatile	1	U_IDRAC9_DRAM1	8 Gb
System CPLD RAM	Volatile	1	U_CPLD1	432 Kb
System CPLD RAM	Non-Volatile	1	U_CPLD1	448 Kb
System Memory	Volatile	Up to 4 per CPU	CPU: A1,A2,A3,A4	Up to 32 GB per DIMM
CPU Vcore and VSA Regulators	Non-Volatile	1 for CPU1,	PU1	16KB
Memory VDDQ Regulators	Non-Volatile	1 for CPU1,	PU30	N/A
4 x 3.5" SAS/SATA front Backplane				
SEP internal flash	Non-Volatile	1	U46	4Mbit in-chip SPI Serial Flash
Backplane External FRU	Non-Volatile	1	U46	256 Bytes
8 x 2.5" SAS/SATA front Backplane				
SEP internal flash	Non-Volatile	1	U46	4Mbit in-chip SPI Serial Flash
Backplane External FRU	Non-Volatile	1	U46	256 Bytes
H755/H755N fPERC (Internal Controller)				
SDRAM	Volatile	9	U1077~U1085	8GB
NV Flash	Non-volatile	1	U1100	512Gb
BMU	Non-Volatile	1	U1126	180KB
SPI Flash	Non-Volatile	1	U1086	128Mb
NVSRAM	Non-volatile	1	U1087	128KB

FRU	Non-volatile	1	U1019	2Kb
SPD	Non-volatile	1	U22	2Kb
CPLD	Non-volatile	1	U1088	64kb
MCU (Cordova)	Non-volatile	1	U41	8KB
H345 fPERC (Internal Controller)				
SPI Flash	Non-Volatile	1	U2	256Mb
NVSRAM	Non-volatile	1	U5	128KB
CPLD	Non-volatile	1	U7	24Kb
FRU	Non-volatile	1	U8	64Kb
RMC	Non-volatile	1	U9	64Kb
MCU (Cordova)	Non-volatile	1	U41	8KB
HBA355i fPERC (Internal controller)				
SPI Flash	Non-Volatile	1	U2	128Mb
FRU	Non-volatile	1	U5	2Kb
CPLD	Non-volatile	1	U23	24kb
MCU	Non-volatile	1	U41	8KB
HBA355E Adapter PERC (External controller)				
SPI Flash	Non-Volatile	1	U2	128Mb
FRU	Non-volatile	1	U5	2Kb
CPLD	Non-volatile	1	U23	24kb
TPM				
Trusted Platform Module (TPM)	Non-Volatile	1	J_TPM1	128 Bytes
BOSS				
RAID controller external SPI FLASH	Non-Volatile	1	U17	8Mb
CPLD	Non-Volatile	1	U1120	256Kb
MCU (Cordova)	Non-volatile	1	U1113	8KB
FRU	Non-Volatile	1	U_BOSS_EEPROM	2Kb
PSU				
DELTA PSU				
MCU	Non-volatile	2	NA	64KB

EEPROM	Non-volatile	1	NA	2KB
LOM				
SPI FLASH	Non-volatile	1	U2001	8Mb

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 Data ROM SPI Flash	SPI Flash	No	4MB Data SPI ROM storage BIOS setting.
iDRAC SPI Flash	SPI Flash	No	iDRAC Uboot (boot loader), server management persistent store (i.e. iDRAC boot variables), and virtual planar FRU
BMC EMMC	eMMC NAND Flash	No	Operational iDRAC FW, Lifecycle Controller (LC) USC partition, LC service diags, LC OS drivers, USC firmware, IDRAC MAC Address, and EPPID, rac log, System Event Log, lifecycle log cache
iDRAC DDR4	RAM	Yes	iDRAC RAM
System CPLD RAM	RAM	No	Not utilized
System Memory	RAM	Yes	System OS RAM
Memory VDDQ, CPU Vcore and VSA Regulators	OTP (one time programmable)	No	Operational parameters
4 x 3.5"; 8 x 2.5" SAS/SATA			
SEP internal flash	Integrated Flash+EEPROM	No	Firmware + FRU
Backplane External FRU	I2C EEPROM	No	FRU
H345/H745/H755/H755N fPERC (Internal controller)			
NVSRAM	NVSRAM	No	Configuration data
FRU	EEPROM	No	Card manufacturing information
SPD	EEPROM	No	Memory configuration data
NV Flash	SPI Flash	No	Card firmware
CPLD	Flash	No	Power sequencing and Cache Offload
SPI Flash	SPI Flash	No	Holds cache data during power loss

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)
SDRAM	SDRAM	No	Cache for HDD I/O
MCU (Cordova)	EEPROM	No	PCIe Bifurcation information to system iDRAC
BMU	Integrated Flash+EEPROM	No	Battery Management control
HBA355i fPERC (Internal controller)			
FRU	EEPROM	No	Card manufacturing information
SPI Flash	SPI Flash	No	Card firmware
CPLD	Flash	No	Power sequencing and Cache Offload
MCU (Cordova)	EEPROM	No	PCIe Bifurcation information to system iDRAC
HBA355E Adapter PERC (External controller)			
FRU	EEPROM	No	Card manufacturing information
SPI Flash	SPI Flash	No	Card firmware
CPLD	Flash	No	Power sequencing and Cache Offload
TPM			
Trusted Platform Module (TPM)	EEPROM	Yes	Storage of encryption keys
IDSDM			
iDSDM (uSD1, uSD2)	NAND Flash	Yes	Provides mass storage
SPI Flash	SPI Flash	SPI flash 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
FRU	FLASH EEPROM	No	Card manufacturing information
PSU			
MCU	Internal Flash	Yes	Boot code, FW
FRU	EEPROM	No	PSU information
LOM			
SPI FLASH	SPI Flash EEPROM	Yes	Firmware

Item	How is data input to this memory?	How is this memory write protected?	How is the memory cleared?
Planer			

Item	How is data input to this memory?	How is this memory write protected?	How is the memory cleared?
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 PCH	Software write protected	Not possible with any utilities or applications and system is not functional if corrupted or removed.
BIOS Data 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.
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 protected	Can be cleared in the system OS
4 x 3.5"; 8 x 2.5" SAS/SATA			

Item	How is data input to this memory?	How is this memory write protected?	How is the memory cleared?
SEP internal flash	I2C interface via iDRAC	Program write protect bit	The user cannot clear memory.
Backplane External FRU	Programmed at ICT during production.	No write protected	The user cannot clear memory.
H345/H745/H755/H755N fPERC (Internal Controller) and H840 Adapter PERC (External Controller)			
NVSRAM	ROC writes configuration data to NVSRAM	no write protected. Not visible to Host Processor	User cannot clear the memory.
FRU	Programmed at ICT during production.	no write protected	User cannot clear the memory.
SPD	Pre-programmed before assembly	no write protected. Not visible to Host Processor	User cannot clear the memory.
Flash	Pre-programmed before assembly. Can be updated using Dell/LSI tools	no write protected. 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	no write protected. 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 controller BIOS and selecting Discard Preserved Cache.
SDRAM	ROC writes to this memory - using it as cache for data IO to HDDs	no write protected. Not visible to Host Processor	Cache can be cleared by powering off the card
HBA355i fPERC (Internal Controller) and HBA355E Adapter PERC (External Controller)			
NVSRAM	ROC writes configuration data to NVSRAM	no write protected. Not visible to Host Processor	User cannot clear the memory.
FRU	Programmed at ICT during production.	no write protected	User cannot clear the memory.
Flash	Pre-programmed before assembly. Can be updated using Dell/LSI tools	no write protected. Not visible to Host Processor	User cannot clear the memory.
TPM			
Trusted Platform Module (TPM)	Using TPM Enabled operating systems	SW write protected	F2 Setup option
IDSDM			
iDSDM (uSD1, uSD2)	device resides in host domain; they are exposed to the user via an internally connected, non-removable USB mass storage device	physical write protect switch on ACE card	(1) card may be physically removed and destroyed or cleared via standard 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	iDRAC may issue a clear command to erase all contents of the SPI NOR, but doing this will leave

Item	How is data input to this memory?	How is this memory write protected?	How is the memory cleared?
		of the primary IDSDM firmware region.	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
PSU			
MCU	The data is flash via Dell Update Package(DUP)	SW write protected	Before firmware update, the memory will be clear.
FRU	During Manufacturing, by programming the image via firmware update process	SW write protected	User cannot clear the memory.
LOM			
SPI FLASH	The data is flash via Dell Update Package(DUP)	Reserving write protection function for HW design.	User cannot clear the memory.

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

10 - 2021