Statement of Volatility – Dell EMC PowerEdge R940

The Dell EMC PowerEdge R940 contain 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 components are present in the PowerEdge R940 servers.

Item	Non-Volatile or Volatile	Quantity	Reference Designator	Size	Type	Can user programs or operating system write data during normal operation?	Purpose	How is data added to the memory?	How is the memory write protected?	How is the memory cleared?
Planar										
PCH Internal CMOS RAM	Non-Volatile	1	U_PCH	256 Bytes	Battery-backed CMOS RAM	No	Real-time clock and BIOS configuration settings	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 Password	Non-Volatile	1	U_PCH	256 bytes	Battery-backed CMOS RAM	Yes	Password to change BIOS settings	Keyboard	N/A	1) Place shunt on J_PSWD_NVRAM jumper pins 2 and 4 2) AC power off is required after placing the shunt. 3) AC power on with the shunt in place and then can be removed

Primary BIOS SPI Flash	Non-Volatile	1	U_SPI_BIOS	32 MB	SPI Flash	No	Boot code	SPI interface via PCH	Software write protected	Not possible with any utilities or applications and system is not functional if corrupted or removed
iDRAC SPI Flash	Non-Volatile	1	U_UBOOT	4 MB	SPI Flash	No	iDRAC Uboot (bootloader)	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	Non-Volatile	1	U_EMMC	4 MB	eMMC NAND Flash	No	Operational iDRAC FW, Lifecycle Controller (LC) USC partition, LC service diags, LC OS drivers, USC firmware	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
CPU Vcore Regulators	Non-Volatile	2	EU_CPU1_VR EU_CPU2_VR	16 KB	ROM	No	Operational parameters	Programmed at factory via I2C	No write protect	The user cannot clear memory completely
Vmem Regulators	Non-Volatile	2	EU_CPU1_VDDQ_VR EU_CPU2_VDDQ_VR	16 KB	ROM	No	Operational parameters	Programmed at factory via I2C	No write protect	The user cannot clear memory completely

System CPLD RAM	Volatile	1	U_CPLD1	92 KB	RAM	No	Power on System Firmware	Firmware update	BIOS Security Protocols	Vendor is Lattice and the programming tool is called Diamond
System CPLD FLASH	Non-Volatile	1	U_CPLD1	256 KB	FLASH	No	Not utilized	Not utilized	Not accessible	Not accessible
System Memory: RDIMM and LRDIMM	Volatile	Up to 12 per CPU	CPU<2:1>_CH<3:0>_D<2:0>	Up to 128 GB per DIMM	DRAM	Yes	System OS RAM	System OS	OS Control	Reboot or power down system
System Memory: NVDIMM M-N	Non-Volatile	Up to 6 per CPUs 1 and 2 (12 total in system)	CPU<2:1>_CH<3:0>_D<2:0>	16GB per NVDIMM-N	Flash – NVDIMM	No	Data integrity	When system initiates a Save (AC loss, shutdown, etc.), NVDIMM-N controller will transfer data from DRAM to Flash	Neither system nor OS can access the flash, only a system initiated Save will trigger the NVDIMM-N controller to transfer data from DRAM to flash	Using BIOS menu option, select NVDIMM factory reset
Internal USB Key	Non-Volatile	Up to 1	J_USB_INT	Varies (not factory installed)	FLASH	Yes	General purpose USB key drive	USB interface via PCH. Accessed via system OS	No write protect	Can be cleared in system OS
CPU	Volatile	1 or 2	CPU1 / CPU2	Various	Cache + registers	Yes	Processor cache + registers	Various	Various	Power off
iDRAC DDR	Volatile	1	U_IDRAC_MEM	256 MB	DRAM	No	iDRAC local memory	iDRAC Firmware	No write protect	Power off
iDRAC	Volatile	1	U_IDRAC	64 kbyte + registers	Cache + registers	No	Processor cache + registers	iDRAC Firmware	No write protect	Power off
CPU PIROM	Non-Volatile	1 or 2	CPU1 / CPU2	256 Bytes	EEPROM	No	Processor info + scratchpad	SMBus interface to iDRAC	128 bytes protected by Intel/128 bytes not protected	Cannot be cleared by the user

Recovery BIOS SPI	Non-Volatile	1	U_REC_SPI_BIOS	16 MB	SPI Flash	No	Recovery image	SPI interface via iDRAC	No write protect	Cannot be cleared by the user
Processor Expansion Module (PEM)										
PEM FRU image	Non-Volatile	1	U_FRU	512 Bytes	I2C EEPROM	No	FRU	I2C interface via expander	Hardware strapping	Cannot be cleared by the user
CPU Vcore Regulators	Non-Volatile	2	EU_CPU3_VR EU_CPU4_VR	16 KB	ROM	No	Operational parameters	Programmed at factory via I2C	No write protect	Cannot be cleared by the user
Vmem Regulators	Non-Volatile	2	EU_CPU3_VDDQ_VR EU_CPU4_VDDQ_VR	16 KB	ROM	No	Operational parameters	Programmed at factory via I2C	No write protect	Cannot be cleared by the user
CPU PIROM	Non-Volatile	1 or 2	CPU3 / CPU4	256 Bytes	EEPROM	No	Processor info + scratchpad	SMBus interface to iDRAC	128 Bytes protected by Intel/128 bytes not protected	Cannot be cleared by the user
CPU	Volatile	1 or 2	CPU3 / CPU4	Various	Cache + registers	Yes	Processor cache + registers	Various	Various	Various
System Memory: RDIMM and LRDIMM	Volatile	Up to 12 per CPU	CPU<4:3>_CH<3:0>_D<2:0>	Up to 128 GB per DIMM	DRAM	Yes	System OS RAM	System OS	OS Control	Reboot or power off the system
System CPLD RAM	Volatile	1	U_CPLD2	92 KB	RAM	No	Power on System Firmware	Firmware update	BIOS Security Protocols	Vendor is Lattice and the programming tool is called Diamond
System CPLD FLASH	Non-Volatile	1	U_CPLD2	256 KB	FLASH	No	Not utilized	Not utilized	Not accessible	Not accessible

24x2.5" Exp/Backplane										
NVSRAM memory	Non-Volatile	1	U_NVSRAM	1 MB	FLASH	No	FW configuration data	Common Flash memory Interface (CFI)	Hardware strapping	Cannot be cleared by the user
Flash memory	Non-Volatile	1	U_FLASH	128 MB	FLASH	No	Firmware	Common Flash memory Interface (CFI)	Hardware strapping	Cannot be cleared by the user
Expander FRU image	Non-Volatile	1	U_EXP_EEPROM	512 Bytes	I2C EEPROM	No	FRU	I2C interface via expander	Hardware strapping	Cannot be cleared by the user
Backplane FRU image	Non-Volatile	1	U_BP_EEPROM	256 Bytes	I2C EEPROM	No	FRU	I2C interface via iDRAC	Hardware strapping	Cannot be cleared by the user
8x2.5" Backplane										
SEP internal flash	Non-Volatile	1	EU_SEP	Flash:32KB+4KB EEPROM: 1KB SRAM:4KB	Integrated Flash+EEPROM	No	Firmware + FRU	I2C interface via iDRAC	Program write protect bit	Cannot be cleared by the user
H730P, H740P, H840 PERCs										
NVSRAM memory	Non-Volatile	1	U1087	128 KB	NVSRAM	No	Configuration data	ROC writes configuration data to NVSRAM	No write protect. Not visible to Host Processor	Cannot be cleared with existing tools available to the customer
FRU	Non-Volatile	1	U1019	256 Bytes	FRU	No	Card manufacturing information	Programmed at ICT during production	No write protect	Cannot be cleared with existing tools available to the customer

SPD	Non-Volatile	1	U22	256 Bytes	SPD	No	Memory configuration data	Pre-programmed before assembly	No write protect. Not visible to Host Processor	Cannot be cleared with existing tools available to the customer
FLASH	Non-Volatile	1	U1086	16 MB	FLASH	No	Card firmware	Pre-programmed before assembly. Can be updated using Dell/LSI tools	No write protect. Not visible to Host Processor	Cannot be cleared with existing tools available to the customer
Backup Flash	Non-Volatile	1	U1100	8 GB	Backup Flash	No	Holds cache data during power loss	FPGA backs up DDR data to this device in case of a power failure	No write protect. 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	Volatile	9	U1077-U1085	8 GB	SDRAM	No	Cache for HDD I/O	ROC writes to this memory - using it as cache for data IO to HDDs	No write protect. Not visible to Host Processor	Cannot be cleared with existing tools available to the customer
H330 PERC										
NVSRAM	Non-volatile	1	U1033	128 KB	NVSRAM	No	Configuration data	ROC writes configuration data to NVSRAM	No write protect. Not visible to Host Processor	Cannot be cleared with existing tools available to the customer
FRU	Non-volatile	1	U1019	256 Bytes	FRU	No	Card manufacturing information	Programmed at ICT during production.	No write protect. Not visible to Host Processor	Cannot be cleared with existing tools available to the customer
1-Wire EEPROM	Non-volatile	1	U1004	128 Bytes	1-Wire EEPROM	No	Holds default controller properties/settings	ROC writes data to this memory	No write protect. Not visible to Host Processor	Cannot be cleared with existing tools available to the customer

Serial Boot ROM	Non-volatile	1	U1020	8 KB	Serial Boot ROM	No	Boot loader	Pre-programmed before assembly	No write protect. Not visible to Host Processor	Cannot be cleared with existing tools available to the customer
Flash	Non-volatile	1	U3	16 MB	FLASH	No	Card firmware	Pre-programmed before assembly. Can be updated using Dell/LSI tools updated using Dell/LSI tools	No write protect. Not visible to Host Processor	Cannot be cleared with existing tools available to the customer
PCIe SSD Extension Card										
Switch Configuration EEPROM	Non-volatile	1	U2	256 Bytes	SPI Flash EEPROM	No (requires specialized SW)	Configuration for PLX PCIe switch, setting register	The EEPROM image is pre-loaded at factory before assembly. Once assembled on the card, data can be entered via PLX Device Editor or PLX EEP DOS based tool.	Device can be write protected via hardware pin. Alternatively, device contents can be write protected via WPEN bit in status register	System is not functional as intended if corrupted/removed
Left Control Panel with Quick Sync 2										
Microcontroller	Non-Volatile	1	USAM7	32 MB	SPI Flash	No	For field maintenance. Have License, Service Tag and	SPI interface via iDRAC	Hardware strapping	Cannot be cleared by the user

							system information.			
TPM										
Trusted Platform Module (TPM)	Non-Volatile	1	U_TPM	128 Bytes	EEPROM	Yes	Storage of encryption keys	Using TPM Enabled operating systems	SW write protected	F2 Setup option
Right Control Panel										
SPI Flash	Non-Volatile	1	U_RGT_CP_SPI	32 MB	SPI Flash	No	EasyRestore functionality: contains Service Tag, Copy of SEL logs	SPI interface from iDRAC to Right Cntl Panel	Embedded iDRAC subsystem firmware actively controls sub area based write protection as needed	Not user clearable, it stays with the system when Motherboard is replaced
FRU	Non-Volatile	1	J_FRU	256 Bytes	FRU	No	Card manufacturing information	Programmed at ICT during production	No write protect	Cannot be cleared with existing tools available to the customer
IDSDM/vFlash										
vFlash (uSD)	Non-Volatile	1	J3	16 GB	NAND flash	Yes	Populate out-of-band, optionally connected to the host mass storage and boot mechanism	User can provide data to iDRAC (entirely in the iDRAC domain) to be pushed into vFlash	no write protect	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 any may clear it manually
uSD1, uSD2	Non-Volatile	2	J1, J2	16 GB, 32 GB, 64 GB	NAND flash	Yes	Provides mass storage	device resides in host domain; they are exposed to the user via an	physical write protect switch on IDSDM/vFLASH card	User has access to the card in the host domain any may clear it manually

								internally connected, non-removable USB mass storage device		
SPI Flash	Non-Volatile	1	U2	1 MB	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.	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	Non-Volatile	1	U17	1024 KB	FLASH EEPROM	No	Boot code, FW	By programming the image via firmware update process	N/A	Use Flash tool, type “go.nsh w y”
TFRU	Non-Volatile	1	U7	64 KB	FLASH EEPROM	Yes	Thermal monitoring	1)During Manufacturing, by programming the image via firmware update process	N/A	By writing to Flash

								2)During runtime, by I2C Proprietary Command Protocol		
PSU										
Microcontroller	Non-Volatile	Up to 3	Microchip	Up to 64 KB	Flash PROM and EEPROM	Yes	Report PSU information and control firmware	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

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