PowerEdge T640 – Informationsaktualisierung – Technisches Datenblatt

Juni 2022
Rev. 1

Hinweise, Vorsichtshinweise und Warnungen

ANMERKUNG: Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, mit denen Sie Ihr Produkt besser einsetzen können.

VORSICHT: Ein VORSICHTSHINWEIS warnt vor möglichen Beschädigungen der Hardware oder vor Datenverlust und zeigt, wie diese vermieden werden können.

WARNUNG: Mit WARNUNG wird auf eine potenziell gefährliche Situation hingewiesen, die zu Sachschäden, Verletzungen oder zum Tod führen kann.

Inhaltsverzeichnis

1

Übersicht

Die Informationen in diesem Dokument ersetzen die Informationen in den entsprechenden Abschnitten des Installations- und Service-Handbuchs Referenzhandbuchs für BIOS und UEFI und der Technischen Daten.

Eine vollständige Liste der Informationen finden Sie in den Dokumenten unter https://www.dell.com/poweredgemanuals.

2

Informationsaktualisierung

Themen:

Anschlüsse auf der Rückwandplatine

Je nach Konfiguration unterstützt das System eine der folgenden Kombinationen von Festplatten:

- 8 x 3,5-Zoll-SAS/SATA-Rückwandplatinen
- 18 x 3,5-Zoll-SAS/SATA-Rückwandplatinen
- 8 x 2,5-Zoll-Rückwandplatine für Dell PowerEdge Express Flash (NVMe)
- 16 x 2,5-Zoll-SAS/SATA-Rückwandplatine mit den optionalen zusätzlichen Rückwandplatinen unten:
  - Rückwandplatine für 8 x 2,5-Zoll-NVMe
  - 16 x 2,5-Zoll-SAS/SATA-Rückwandplatinen (FlexBay)
- 32 x 2,5-Zoll-SAS/SATA-Rückwandplatinen

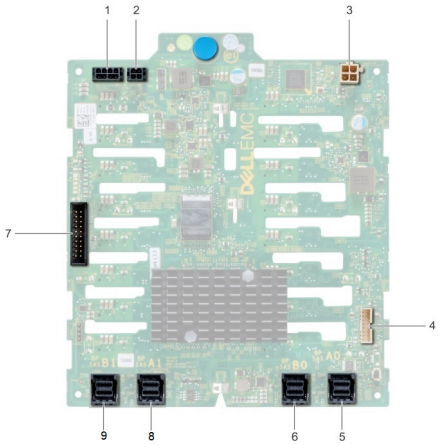

Abbildung 1. 16 x 2,5-Zoll-SAS/SATA-Rückwandplatine für FlexBay (oben)

1. Stromanschluss A der Rückwandplatine [J_BP_PWR_A]
2. Stromanschluss B der Rückwandplatine [J_BP_PWR_B]
3. Stromanschluss für optisches Laufwerk [J_ODD_PWR]
4. Signalanschluss für Rückwandplatine [J_BP_SIG]
5. SAS A0-Anschluss [J_SAS_A0]
6. SAS B0-Anschluss [J_SAS_B0]
7. I2C-Anschluss
8. SAS A1-Anschluss [J_EXP_A1]
9. SAS B1-Anschluss [J_EXP_B1]

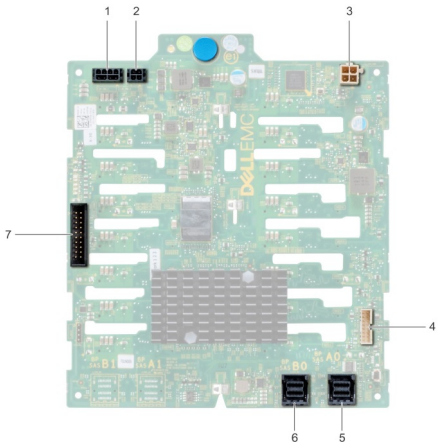

Abbildung 2. 16 x 2,5-Zoll-SAS/SATA-Rückwandplatinen (unten)

1. Stromanschluss A der Rückwandplatine [J_BP_PWR_A]
2. Stromanschluss B der Rückwandplatine [J_BP_PWR_B]
3. Stromanschluss für optisches Laufwerk [J_ODD_PWR]
4. Signalanschluss für Rückwandplatine [J_BP_SIG]
5. SAS A0-Anschluss [J_SAS_A0]
6. SAS B0-Anschluss [J_SAS_B0]
7. I2C-Anschluss

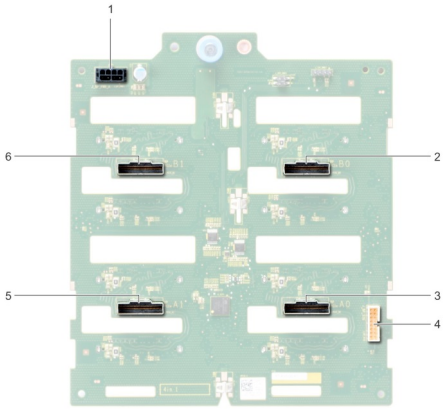

Abbildung 3. Rückwandplatine für 8 x 2,5-Zoll-NVMe

1. Netzanschluss der Rückwandplatine [J_BP_PWR1]
2. PCIe B0-Anschluss [J_PCIE_B0]
3. PCIe A0-Anschluss [J_PCIE_A0]
4. Signalanschluss für Rückwandplatine [J_BP_SIG1]
5. PCIe A1-Anschluss [J_PCIE_A1]
6. PCIe B1-Anschluss [J_PCIE_B1]

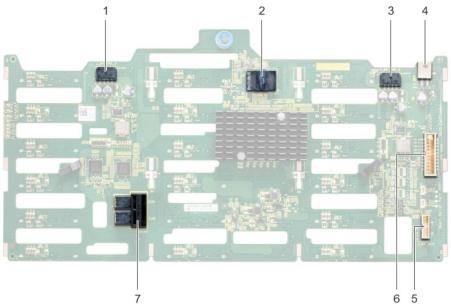

Abbildung 4. 18 x 3,5-Zoll-SAS/SATA-Rückwandplatinen

1. Stromanschluss A der Rückwandplatine [J_BP_PWR_A1]
2. Controller
3. Stromanschluss B der Rückwandplatine [J_BP_PWR_B1]
4. Stromanschluss für optisches Laufwerk [J_ODD1]
5. I2C-Anschluss
6. Signalanschluss für Rückwandplatine [J_BP_SIG1]
7. SAS A0_B0-Anschluss [J_SAS_A0_B0]

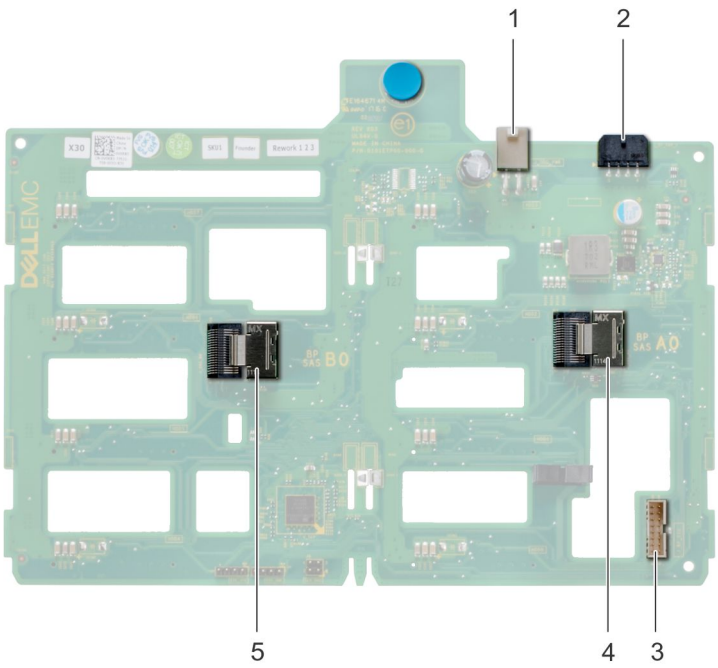

Abbildung 5. 8 x 3,5-Zoll-SAS/SATA-Rückwandplatinen

1. Stromanschluss für optisches Laufwerk [J_ODD1]
2. Netzanschluss der Rückwandplatine [J_BP_PWR_A]
3. SAS A0-Anschluss [J_BP_SIG]
4. Signalanschluss für Rückwandplatine [J_SAS_A0]
5. SAS B0-Anschluss [J_SAS_B0]

Systemsicherheit

Mit dem Bildschirm **System Security** (Systemsicherheit) können Sie bestimmte Funktionen wie das Festlegen des Kennworts des System, des Setup-Kennworts und die Deaktivierung des Betriebsschalters durchführen.

Anzeigen von „System Security“ (Systemsicherheit)

Führen Sie folgenden Schritte durch, um den Bildschirm **System Security** (Systemsicherheit) anzuzeigen:

Schritte

1. Schalten Sie das System ein oder starten Sie es neu.
2. Drücken Sie umgehend auf die Taste <F2>, wenn die folgende Meldung angezeigt wird:

```
F2 = System Setup
```

ANMERKUNG: Wenn der Ladevorgang des Betriebssystems beginnt, bevor Sie F2 gedrückt haben, lassen Sie das System den Startvorgang vollständig ausführen. Starten Sie dann das System neu und versuchen Sie es erneut.

3. Klicken Sie auf dem Bildschirm **System Setup Main Menu** (System-Setup-Hauptmenü) auf **System BIOS** (System-BIOS).
4. Klicken Sie auf dem Bildschirm **System BIOS** (System-BIOS) auf **System Security** (Systemsicherheit).

Details zum Bildschirm „Systemsicherheitseinstellungen“

Info über diese Aufgabe

Die Details zum Bildschirm **System Security Settings** (Systemsicherheitseinstellungen) werden nachfolgend erläutert:

Option	Beschreibung
CPU AES-NI	Verbessert die Geschwindigkeit von Anwendungen durch Verschlüsselung und Entschlüsselung unter Einsatz der AES-NI-Standardanweisungen und ist per Standardeinstellung auf Enabled (Aktiviert) gesetzt. In der Standardeinstellung ist diese Option auf **Enabled** (Aktiviert).
System Password	Ermöglicht das Einrichten des Systemkennworts. Diese Option ist standardmäßig auf **Enabled** (Aktiviert) gesetzt und ist schreibgeschützt, wenn der Jumper im System nicht installiert ist.
Setup-Kennwort	Ermöglicht das Einrichten des System-Setup-Kennworts. Wenn der Kennwort-Jumper nicht im System installiert ist, ist diese Option schreibgeschützt.
Kennwortstatus	Ermöglicht das Sperren des Systemkennworts. In der Standardeinstellung ist diese Option auf **Unlocked** (Entriegelt).
TPM Security	**ANMERKUNG:** Das TPM-Menü ist nur verfügbar, wenn das TPM-Modul installiert ist. Ermöglicht es Ihnen, den Berichtsmodus des TPMs zu steuern. Standardmäßig ist die Option **TPM Security** (TPM-Sicherheit) auf **Off** (Deaktiviert) eingestellt. Die Felder „TPM Status“ (TPM-Status), „TPM Activation“ (TPM-Aktivierung) und „Intel TXT“ können nur geändert werden, wenn das Feld **TPM Status** (TPM-Status) auf **On with Pre-boot Measurements** (Aktiviert mit Maßnahmen vor dem Start) oder **On without Pre-boot Measurements** (Aktiviert ohne Maßnahmen vor dem Start) gesetzt ist.
TPM-Informationen	Ermöglicht das Ändern des TPM-Betriebszustands. Diese Option ist standardmäßig auf **Type: 2.0-NTZ** eingestellt.
TPM Status	Gibt den TPM-Status an.
TPM-Befehl	Setzen Sie das TPM (Trusted Platform Module) ein. Bei der Einstellung **Keine** wird kein Befehl an das TPM gesendet. Bei der Einstellung **Aktivieren** ist das TPM aktiviert. Bei der Einstellung **Deactivate (Deaktivieren)**, ist das TPM deaktiviert. Bei der Einstellung **löschen**, werden alle Inhalte des TPM gelöscht. In der Standardeinstellung ist diese Option auf **None** (Keine). **VORSICHT: Das Löschen des TPM führt zum Verlust aller Schlüssel im TPM. Der Verlust von TPM-Schlüsseln kann den Startvorgang des Betriebssystems beeinträchtigen.** Dieses Feld ist schreibgeschützt, wenn **TPM Security** auf **Off**. Diese Aktion erfordert einen zusätzlichen Neustart, bevor sie wirksam wird.
TPM Hierarchy	Ermöglicht das Aktivieren, Deaktivieren oder Löschen von Speicher- und Endorsement Key-Hierarchien. Wenn diese Einstellung auf **Enabled** (Aktiviert) festgelegt ist, können die Speicher- und Endorsement Key-Hierarchien verwendet werden. Wenn diese Einstellung auf **Disabled** (Deaktiviert) festgelegt ist, können die Speicher- und Endorsement Key-Hierarchien nicht verwendet werden. Wenn diese Einstellung auf **Clear** (Löschen) festgelegt ist, werden alle Werte aus den Speicher- und Endorsement Key-Hierarchien gelöscht. Anschließend wird die Einstellung auf **Enabled** (Aktiviert) festgelegt.
Erweiterte TPM-Einstellungen	Diese Einstellung ist nur aktiviert, wenn TPM Security auf „On“ gesetzt ist.
Intel(R) TXT	Ermöglicht das Aktivieren bzw. Deaktivieren der Option „Intel Trusted Execution Technology (TXT)“. Zur Aktivierung von **Intel TXT** muss die Virtualisierungstechnologie aktiviert werden und die TPM-Sicherheit mit Vorstart-Messungen auf Enabled (Aktiviert) gesetzt werden. In der Standardeinstellung ist diese Option auf **Off** (Aus).
Netzschalter	Ermöglicht das Aktivieren bzw. Deaktivieren des Netzschalters auf der Vorderseite des Systems. In der Standardeinstellung ist diese Option auf **Enabled** (Aktiviert).
Netzstromwiederherstellung	Ermöglicht das Festlegen der Reaktion des Systems, nachdem die Netzstromversorgung des System wiederhergestellt wurde. In der Standardeinstellung ist diese Option auf **Last** (Letzte).
Verzögerung bei Netzstromwiederherstellung	Ermöglicht das Einstellen der Zeitspanne, die für das Hochfahren des Systems in Anspruch genommen werden soll, nachdem die Netzstromversorgung des System wiederhergestellt wurde. In der Standardeinstellung ist diese Option auf **Immediate** (Sofort).
User Defined Delay (Benutzerdefinierte Verzögerung) (60 bis 600 s)	Ermöglicht das Festlegen der Option **User Defined Delay** (Benutzerdefinierte Verzögerung), wenn für **AC Power Recovery Delay** (Verzögerung bei Netzstromwiederherstellung) die Option **User Defined** (Benutzerdefiniert) gewählt wird.

Option	Beschreibung
Variabler UEFI-Zugriff	Bietet unterschiedliche Grade von UEFI-Sicherungsvariablen. Wenn die Option auf **Standard** (Standardeinstellung) gesetzt ist, sind die UEFI-Variablen gemäß der UEFI-Spezifikation im Betriebssystem aufrufbar. Wenn die Option auf **Controlled** (Kontrolliert) gesetzt ist, werden die ausgewählten UEFI-Variablen in der Umgebung geschützt und neue UEFI-Starteinträge werden an das Ende der aktuellen Startreihenfolge gezwungen.
In-Band Benutzeroberfläche	Bei der Einstellung **Disabled** (Deaktiviert), blendet diese Einstellung der Management Engine (ME), HECI Geräte und des Systems IPMI-Geräte aus dem Betriebssystem aus. Dadurch wird verhindert, dass der Betriebssystem vom Ändern des ME Power Capping Einstellungen und blockiert den Zugriff auf alle In-Band -Management Tools. Alle Management verwaltet werden sollte über Out-of-Band-. In der Standardeinstellung ist diese Option auf **Enabled** (Aktiviert). **ANMERKUNG:** BIOS-Aktualisierung erfordert HECI Geräte in Betrieb sein und DUP Aktualisierungen erfordern IPMI-Schnittstelle in Betrieb sein. Diese Einstellung muss so eingestellt werden **Aktiviert** zu vermeiden Aktualisierungsfehler.
Secure Boot	Ermöglicht den sicheren Start, indem das BIOS jedes Vorstart-Image mit den Zertifikaten in der Sicherungsstartrichtlinie bzw. Regel für sicheren Start authentifiziert. „Secure Start“ (Sicherer Start) ist in der Standardeinstellung deaktiviert. Sicherer Start ist standardmäßig auf **Standard** festgelegt.
Regel für sicheren Start	Wenn die Richtlinie für den sicheren Start auf **Standard** eingestellt ist, authentifiziert das BIOS die Vorstart-Images mithilfe des Schlüssels und der Zertifikate des Systemherstellers. Wenn die Richtlinie für den sicheren Start auf **Custom** (Benutzerdefiniert) eingestellt ist, verwendet das BIOS benutzerdefinierte Schlüssel und Zertifikate. Die Richtlinie für den sicheren Start ist standardmäßig auf **Standard** festgelegt.
Secure Boot Mode	Ermöglicht es Ihnen, festzulegen, wie das BIOS die Objekte der Regel für sicheren Start (PK, KEK, db, dbx) verwendet. Wenn der aktuelle Modus eingestellt ist zum **Modus „Bereitgestellt“**, die verfügbaren Optionen sind **Benutzermodus** und **Modus „Bereitgestellt“**. Wenn die aktuelle Modus ist **Benutzermodus**, die verfügbaren Optionen sind **Benutzermodus**, **Prüfmodus**, und **Modus „Bereitgestellt“**.

Optionen	Beschreibung
Benutzermodi	Im **Benutzermodus**, PK muss installiert sein, und das BIOS führt die Signaturüberprüfung auf programmatischer versucht, Regel zum Aktualisieren Objekte. Das BIOS lässt unbestätigte programmgesteuerte Übergänge zwischen Modi zu.
Audit Modus	Im **Prüfmodus**, PK ist nicht vorhanden. Das BIOS bestätigt programmgesteuerte Aktualisierungen der Richtlinienobjekte und Übergänge zwischen den Modi nicht. **Audit Modus** eignet sich für programmgesteuert zur Festlegung einer arbeiten Satz von Richtlinie Objekte. Das BIOS führt eine Signaturüberprüfung der Vorstart-Images durch. Das BIOS protokolliert auch die Ergebnisse in der Ausführungsinformationen-Tabelle der Images, wobei die Images zugelassen werden, unabhängig davon, ob sie die Prüfung bestanden haben oder nicht.
Modus Bereitgestellt	**Modus Bereitgestellt** ist die sicherste Modus. Im **Modus Bereitgestellt**, PK muss installiert sein und der BIOS führt die Signaturüberprüfung auf programmatischer versucht, Regel zum Aktualisieren Objekte. **Modus Bereitgestellt** schränkt die programmatischer Mode-Übergänge.

Richtlinie zum sicheren Start – Übersicht	Gibt die Liste der Zertifikate und Hashes für den sicheren Start an, die beim sicheren Start für authentifizierte Images verwendet werden.
Benutzerdefinierte Einstellungen für die Richtlinie zum sicheren Start	Konfiguriert die Secure Boot Custom Policy. Zur Aktivierung dieser Option müssen Sie **Secure Boot Policy** (Secure Boot-Richtlinie) auf **Custom** (Benutzerdefiniert) setzen.