Mise à jour des informations sur le système PowerEdge T640 - Fiche technique

Juin 2022
Rév. 1

DELL Technologies

Remarques, précautions et avertissements

REMARQUE : Une REMARQUE indique des informations importantes qui peuvent vous aider à mieux utiliser votre produit.

PRÉCAUTION : Une PRÉCAUTION indique un risque d'endommagement du matériel ou de perte de données et vous indique comment éviter le problème.

AVERTISSEMENT : Un AVERTISSEMENT indique un risque d'endommagement du matériel, de blessures corporelles ou même de mort.

Table des matières

1

Présentation

Les informations contenues dans ce document remplacent celles fournies dans les sections pertinentes des documents suivants : Manuel d'installation et de maintenance, Guide de référence du BIOS et de l'UEFI, et Spécifications techniques.

Pour obtenir la liste complète des informations, consultez les documents disponibles sur https://www.dell.com/poweredgemanuals

2

Mise à jour des informations

Sujets :

Connecteurs de fond de panier

Selon la configuration, votre système prend en charge un ou plusieurs éléments suivants :

- 8 fonds de panier SAS/SATA de 3,5 pouces
- 18 fonds de panier SAS/SATA de 3,5 pouces
- 8 fonds de panier Dell PowerEdge Express Flash (NVMe) de 2,5 pouces
- 16 fonds de panier SAS/SATA de 2,5 pouces avec les fonds de panier supplémentaires en option ci-dessous :
  - 8 fonds de panier NVMe de 2,5 pouces
  - 16 fonds de panier SAS/SATA (FlexBay) de 2,5 pouces
- 32 fonds de panier SAS/SATA de 2,5 pouces

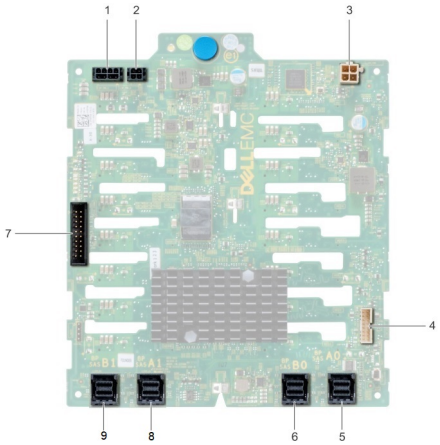

Figure 1. 16 fonds de panier SAS/SATA pour FlexBay (partie supérieure) de 2,5 pouces

1. Connecteur d'alimentation du fond de panier A [J_BP_PWR_A]
2. Connecteur d'alimentation du fond de panier B [J_BP_PWR_B]
3. Connecteur d'alimentation du lecteur optique [J_ODD_PWR]
4. Connecteur de transmission du fond de panier [J_BP_SIG]
5. Connecteur SAS A0 [J_SAS_A0]
6. Connecteur SAS B0 [J_SAS_B0]
7. Connecteur I2C
8. Connecteur SAS A1 [J_EXP_A1]
9. Connecteur SAS B1 [J_EXP_B1]

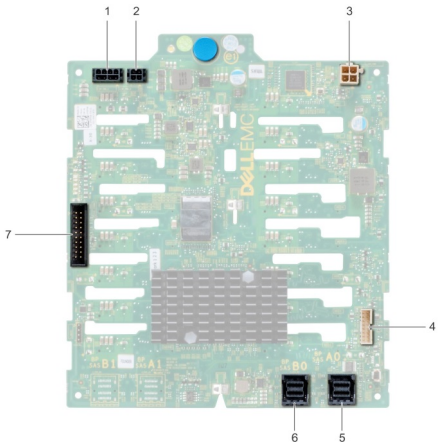

Figure 2. 16 fonds de panier SAS/SATA de 2,5 pouces (partie inférieure)

1. Connecteur d'alimentation du fond de panier A [J_BP_PWR_A]
2. Connecteur d'alimentation du fond de panier B [J_BP_PWR_B]
3. Connecteur d'alimentation du lecteur optique [J_ODD_PWR]
4. Connecteur de transmission du fond de panier [J_BP_SIG]
5. Connecteur SAS A0 [J_SAS_A0]
6. Connecteur SAS B0 [J_SAS_B0]
7. Connecteur I2C

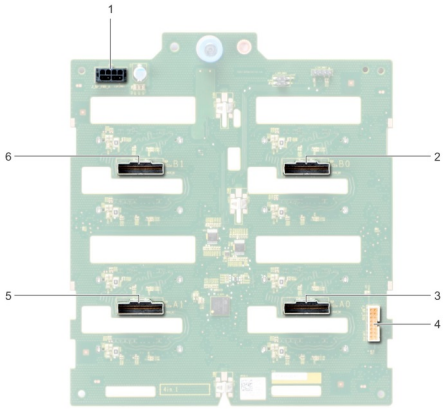

Figure 3. 8 fonds de panier NVMe de 2,5 pouces

1. Connecteur d'alimentation de fond de panier [J_BP_PWR1]
2. Connecteur PCIe B0 [J_PCIE_B0]
3. Connecteur PCIe A0 [J_PCIE_A0]
4. Connecteur de transmission du fond de panier [J_BP_SIG1]
5. Connecteur PCIe A1 [J_PCIE_A1]
6. Connecteur PCIe B1 [J_PCIE_B1]

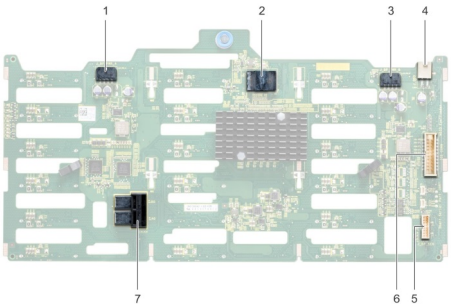

Figure 4. 18 fonds de panier SAS/SATA de 3,5 pouces

1. Connecteur d'alimentation du fond de panier A [J_BP_PWR_A1]
2. contrôleur
3. Connecteur d'alimentation du fond de panier B [J_BP_PWR_B1]
4. Connecteur d'alimentation du lecteur optique [J_ODD1]
5. Connecteur I2C
6. Connecteur de transmission du fond de panier [J_BP_SIG1]
7. Connecteur SAS A0_B0 [J_SAS_A0_B0]

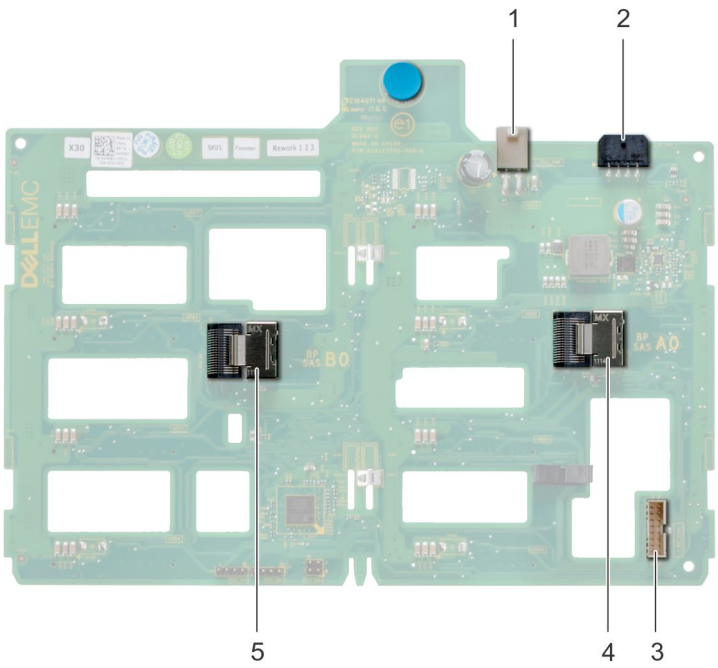

Figure 5. 8 fonds de panier SAS/SATA de 3,5 pouces

1. Connecteur d'alimentation du lecteur optique [J_ODD1]
2. Connecteur d'alimentation du fond de panier [J_BP_PWR_A]
3. Connecteur SAS A0 [J_BP_SIG]
4. Connecteur de transmission du fond de panier [J_SAS_A0]
5. Connecteur SAS B0 [J_SAS_B0]

Sécurité du système

L'écran **Sécurité du système** permet d'exécuter des fonctions spécifiques telles que la définition du mot de passe de l'système et du mot de passe de configuration et la désactivation du bouton d'alimentation.

Affichage de la sécurité du système

Pour afficher l'écran **Sécurité du système**, procédez comme suit :

Étapes

1. Allumez ou redémarrez le système.
2. Appuyez sur F2 dès que vous voyez le message suivant :

```
F2 = System Setup
```

REMARQUE : Si le système d'exploitation commence à se charger alors que vous n'avez pas encore appuyé sur F2 attendez que le système finisse de démarrer, redémarrez-système et réessayez.

3. Dans l'écran **Menu principal de configuration du système**, cliquez sur **BIOS du système**.
4. Sur l'écran **BIOS du système**, cliquez sur **Sécurité du système**.

Informations détaillées Paramètres de sécurité du système

À propos de cette tâche

Le détail de l'écran **Paramètres de sécurité du système** est le suivant :

Option	Description
Processeur AES-NI	Optimise la vitesse des applications en effectuant le chiffrement et le déchiffrement à l'aide d'AES-NI et est Activé par défaut. Par défaut, cette option est définie sur **Activé**.
Mot de passe système	Vous permet de définir le mot de passe système. Cette option est définie sur **Activé** par défaut et est en lecture seule si le cavalier de mot de passe n'est pas installé dans le système.
Mot de passe de configuration	Vous permet de définir le mot de passe de configuration du système. Cette option est en lecture seule si le cavalier du mot de passe n'est pas installé sur le système.
État du mot de passe	Vous permet de verrouiller le mot de passe du système. Par défaut, l'option est définie sur **Déverrouillé**.
Sécurité TPM	**REMARQUE :** Le menu du module TPM n'est disponible que si ce dernier est installé. Permet de contrôler le mode de signalement du module TPM. Par défaut, l'option **Sécurité du module TPM** est réglée sur **Désactivé**. Vous pouvez uniquement modifier les champs d'état du module TPM, d'activation de la puce TPM et d'Intel TXT si le champ **État TPM** est réglé sur **Activé avec les mesures de pré-amorçage** ou **Activé sans mesures pré-amorçage**.
Informations sur le module TPM	Vous permet de modifier l'état opérationnel du module TPM. Par défaut, cette option est réglée sur **Type : 2.0-NTZ**.
État du module TPM	Spécifie l'état du module TPM.
Commande de module TPM	Installez le module TPM (Trusted Platform Module). Lorsqu'elle est définie sur **Aucun**, aucune commande n'est envoyée au module TPM. Lorsqu'elle est définie sur **Activer**, le TPM est activé. Lorsqu'elle est définie sur **Désactiver**, le TPM est désactivé. Lorsqu'elle est définie sur **Effacer**, tout le contenu du module TPM est effacé. Par défaut, l'option est définie sur **Aucun**. **PRÉCAUTION : L'effacement du module TPM entraîne une perte de toutes les clés du module TPM. La perte des clés du module TPM peut affecter le démarrage du système d'exploitation.** Ce champ est en lecture seule lorsque **la sécurité TPM** est définie sur **Désactivé**. Cette action nécessite un redémarrage supplémentaire avant de prendre effet.
Hiérarchie TPM	Permet d'activer, de désactiver ou d'effacer les hiérarchies de stockage et de validation. Lorsque cette option est définie sur **Activé**, les hiérarchies de stockage et de validation peuvent être utilisées. Lorsque cette option est définie sur **Désactivé**, les hiérarchies de stockage et de validation ne peuvent pas être utilisées. Lorsque cette option est définie sur **Effacer**, les valeurs des hiérarchies de stockage et de validation sont effacées, puis l'option est redéfinie sur **Activé**.
Paramètres TPM avancés	Ce paramètre est activé uniquement lorsque la sécurité TPM est activée.
Intel® TXT	Vous permet d'activer l'option Intel Trusted Execution Technology (TXT). Pour activer **Intel TXT**, l'option Technologie de virtualisation doit être activée et l'option Sécurité du module TPM doit être activée avec les mesures de pré-amorçage. Par défaut, l'option est définie sur **Désactivé**.
Bouton d'alimentation	Vous permet d'activer le bouton d'alimentation sur l'avant du système. Par défaut, cette option est définie sur **Activé**.
Restauration de l'alimentation secteur	Vous permet de définir le temps de réaction du système une fois l'alimentation secteur restaurée dans le système. Par défaut, l'option est définie sur **Dernier**.
Délai de restauration de l'alimentation secteur	Vous permet de régler la façon dont le système prend en charge le décalage de mise sous tension une fois l'alimentation secteur restaurée dans le système. Par défaut, l'option est définie sur **Immédiatement**.
Délai défini par l'utilisateur (60 s à 600 s)	Vous permet de régler le paramètre **Délai défini par l'utilisateur** lorsque l'option **Utilisateur défini** de **Délai de restauration de l'alimentation secteur** est sélectionnée.
Accès aux variables UEFI	Fournit différents degrés de protection des variables UEFI. Lorsqu'elle est définie sur **Standard** (par défaut), les variables UEFI sont accessibles dans le système d'exploitation selon la spécification UEFI. Lorsqu'elles sont définies

Option	Description
	sur **contrôlé**, les variables UEFI sélectionnées sont protégées dans l'environnement et de nouvelles entrées d'amorçage UEFI sont obligées d'être à la fin de l'ordre d'amorçage.
Interface de facilité de gestion intrabande	Lorsqu'il est défini sur **Désactivé**, ce paramètre cache le système Management Engine (ME), les appareils HECI et les appareils IPMI du système à partir du système d'exploitation. Cela empêche le système d'exploitation de modifier les paramètres de plafonnement de l'alimentation ME, et bloque l'accès à tous les outils de gestion intrabande. Toutes les fonctions de gestion doivent être gérées par hors bande. Par défaut, cette option est définie sur **Activé**. **REMARQUE :** Mise à jour du BIOS nécessite HECI appareils à être opérationnel et le DUP mises à jour nécessitent interface IPMI pour être opérationnel. Ce paramètre doit être défini sur **Activé** mise à jour afin d'éviter les erreurs.
Secure Boot	Permet d'activer Secure Boot, où le BIOS authentifie chaque image de préamorçage à l'aide des certificats de la stratégie Secure Boot. Par défaut, la stratégie Secure Boot est définie sur **Désactivé** (par défaut).
Politique Secure Boot	Lorsque la stratégie Secure Boot est définie sur **Standard**, le BIOS utilise des clés et des certificats du fabricant du système pour authentifier les images de préamorçage. Lorsque la stratégie Secure Boot est définie sur **Personnalisé**, le BIOS utilise des clés et des certificats définis par l'utilisateur. Par défaut, la stratégie secure Boot est définie sur **Standard**.
Mode Secure Boot	Permet de configurer la façon dont le BIOS utilise les objets de stratégie Secure Boot (PK, KEK, db, dbx). Si le mode actuel est défini sur **mode déployé**, les options disponibles sont **Mode d'utilisateur** et **mode déployé**. Si le mode actuel est défini sur **Mode utilisateur**, les options disponibles sont **Mode utilisateur**, **Mode audit**, et **Mode déployé**.

Options	Description
Mode utilisateur	En **mode utilisateur**, PK doit être installé, et le BIOS effectue vérification de signature sur objets de stratégie programmatique tente de les mettre à jour. Le BIOS permet des transitions programmatiques non authentifiées entre les modes.
Mode audit	En **mode audit**, PK n'est présente. Le BIOS n'authentifie pas les mises à jour programmatiques des objets de stratégie et les transitions entre modes. Le **mode audit** est utile pour définir une plage de travail de programmation par objets de stratégie. Le BIOS effectue la vérification de la signature sur les images de pré-démarrage. Le BIOS enregistre également les résultats dans la table d'information d'exécution d'image, mais approuve les images qu'elles réussissent ou échouent la vérification.
Mode déployé	**Mode déployé** est le plus mode sécurisé. En **mode déployé**, PK doit être installé et le BIOS effectue vérification de signature sur objets de stratégie programmatique tente de les mettre à jour. **Mode déployé** limite les transitions de mode programmé.

Résumé de la stratégie Secure Boot	Spécifie la liste des certificats et des hachages qu'utilise Secure Boot pour authentifier des images.
Paramètres de la politique personnalisée Secure Boot	Configure la stratégie personnalisée Secure Boot. Pour activer cette option, définissez la **Stratégie Secure Boot** sur **Personnalisée**.