Mise à jour des informations sur le système PowerEdge T550 - Fiche technique

Novembre 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 Caractéristiques techniques.

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

Sujets :

Historique des révisions

Cette section décrit les modifications apportées au document.

Tableau 1. Historique des révisions du document

Révision du document	Date	Description des modifications
1	Novembre 2022	1. Mise à jour du BIOS, de la sécurité du système, d'Intel(R) SGX 2. Mise à jour des blocs d'alimentation 3. Mise à jour de la configuration minimale pour l'auto-test de démarrage

2

Configuration minimale pour l’auto-test au démarrage (POST)

- Un processeur dans le processeur à socket 1
- Un module de mémoire (DIMM) dans le socket A1
- Carte intercalaire d’alimentation (PIB) et câbles
- Un bloc d’alimentation
- Carte système

3

Sécurité des systèmes

Pour afficher l'écran **Sécurité des systèmes**, mettez le système sous tension, appuyez sur la touche F2, puis cliquez sur **Menu principal de configuration du système** > **BIOS du système** > **Sécurité des systèmes**.

Tableau 2. Détails de l'écran Sécurité des systèmes

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	Affiche le mot de passe du système. Cette option est réglée 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	Définir le mot de passe de configuration. 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	Permet de verrouiller le mot de passe du système. Par défaut, l'option est définie sur **Déverrouillé**.
Informations TPM	Indique le type de module de plate-forme sécurisé.

Tableau 3. Informations de sécurité du module TPM 1.2

Option		Description
Informations TPM		
Sécurité du module 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 modifier l'État TPM et l'Activation TPM uniquement si le champ **État TPM** est défini sur **Activé avec les mesures de pré-amorçage** ou **Activé sans les mesures de pré-amorçage**. Lorsque le module TPM 1.2 est installé, l'option **Sécurité TPM** est définie sur **Désactivé**, **Activé avec les mesures de pré-démarrage** ou **Activé sans les mesures de pré-démarrage**.
Informations TPM		Affiche l'état opérationnel du TPM.
TPM Firmware		Indique la version du firmware du TPM.
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**.
Paramètres avancés de TPM	**Provision pour dérivation PPI de TPM**	Lorsqu'elle est définie sur **Activé**, cette fonction permet au système d'exploitation d'ignorer les invites de l'interface de présence physique (PPI, Physical Presence Interface) lors des opérations de provisionnement de l'ACPI (Advanced Configuration and Power Interface) PPI.
	Effacement pour dérivation PPI de TPM	Lorsqu'elle est définie sur **Activé**, cette fonction permet au système d'exploitation d'ignorer les invites de l'interface de présence physique (PPI, Physical Presence Interface) lors des opérations de provisionnement de l'ACPI (Advanced Configuration and Power Interface) PPI.

Tableau 4. Informations de sécurité du module TPM 2.0

Option	Description	
Informations TPM		
Sécurité du module 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**. Lorsque l'option TPM 2.0 est installée, la **sécurité de la puce TPM** est réglée sur **Activé** ou **Désactivé**. Par défaut, cette option est définie sur **Désactivé**.	
Informations TPM	Affiche l'état opérationnel du TPM.	
TPM Firmware	Indique la version du firmware du TPM.	
TPM Hierarcy	Active, désactive ou efface 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	**Provision pour dérivation PPI de TPM**	Lorsqu'elle est définie sur **Activé**, cette fonction permet au système d'exploitation d'ignorer les invites de l'interface de présence physique (PPI, Physical Presence Interface) lors des opérations de provisionnement de l'ACPI (Advanced Configuration and Power Interface) PPI.
	Effacement pour dérivation PPI de TPM	Lorsqu'elle est définie sur **Activé**, cette fonction permet au système d'exploitation d'ignorer les invites de l'interface de présence physique (PPI, Physical Presence Interface) lors des opérations de provisionnement de l'ACPI (Advanced Configuration and Power Interface) PPI.
	Sélection de l'algorithme TPM2	Cette option permet à l'utilisateur de modifier les algorithmes cryptographiques utilisés dans le TPM (Trusted Platform Module). Les options disponibles varient en fonction du micrologiciel du TPM. Pour activer la sélection d'algorithmes TPM2, la technologie Intel(R) TXT doit être désactivée. L'option Sélection d'algorithme TPM2 prend en charge SHA1, SHA128, SHA256, SHA512 et SM3 en détectant le module TPM. L'option est réglée sur **SHA1** par défaut.

Tableau 5. Détails de l'écran Sécurité des systèmes (suite)

Option	Description
Intel(R) TXT	Vous permet d'activer l'option Intel Trusted Execution Technology (TXT). Pour activer l'option **Intel TXT**, la technologie de virtualisation et la sécurité TPM doivent être activées avec les mesures de prédémarrage pour le module TPM 1.2 ou définies sur **Activé** avec l'algorithme SHA256 pour le module TPM 2.0. Par défaut, cette option est définie sur **Désactivé**. Elle est définie sur **Activé** pour la prise en charge du démarrage sécurisé (protection du firmware) sous Windows 2022.
Chiffrement de la mémoire	Permet d'activer ou de désactiver le chiffrement de la mémoire totale Intel (TME) et multiclient (Intel® TME-MT). Lorsque l'option est définie sur **Désactivé**, le BIOS désactive la technologie TME et MK-TME. Lorsque l'option est définie sur **Une seule touche**, le BIOS active la technologie TME. Lorsque l'option est définie sur **Plusieurs clés**, le BIOS active la technologie TME-MT, l'option Limite d'adresse physique du processeur doit être désactivée pour sélectionner l'option Plusieurs clés. Par défaut, cette option est définie sur **Désactivé**.
Intel(R) SGX	Permet d'activer ou de désactiver l'option Intel Software Guard Extension (SGX). Pour activer l'option **Intel SGX**, le processeur doit être doté d'une prise en charge de la fonction SGX. La population de la mémoire doit être compatible (au minimum 8 x DIMM1 identiques à DIMM8 par socket d'UC, pas de prise en charge avec la configuration de mémoire permanente). Le mode de fonctionnement de la mémoire doit être défini en mode optimiseur. Le chiffrement de

Tableau 5. Détails de l'écran Sécurité des systèmes (suite)

Option	Description
	mémoire doit être activé et l'entrelacement de nœuds doit être désactivé. Par défaut, cette option est définie sur **Désactivé**. Lorsque cette option est définie sur **Désactivé**, le BIOS désactive la technologie SGX. Lorsque cette option est définie sur **Activé**, le BIOS active la technologie SGX.
Accès intrabande aux informations sur le package SGX	Permet de bénéficier d'un accès intrabande aux informations sur le package Intel Software Guard Extension (SGX). Par défaut, cette option est définie sur **Désactivé**.
Taille de PPMRR	Cette option permet de définir la taille des registres PPMRR.
QoS SGX	Cette option permet d'activer ou de désactiver la qualité de service SGX.
Sélectionnez le type d'entrée Owner EPOCH	Cette option permet de sélectionner **Passer à de nouveaux Owner EPOCH aléatoires** ou **Owner EPOCH définis manuellement par l'utilisateur**. Chaque Owner EPOCH est à 64 bits. Après avoir généré un nouveau Owner EPOCH en sélectionnant l'option **Passer à de nouveaux Owner EPOCH aléatoires**, la sélection revient sur **Owner EPOCH définis manuellement par l'utilisateur**.
	Software Guard Extensions Epoch n : définit les valeurs Software Guard Extensions Epoch.
Activer les écritures sur SGXLEPUBKEYHASH[3:0] à partir du système d'exploitation/logiciel	Cette option permet d'activer les écritures sur SGXLEPUBKEYHASH[3:0] à partir du système d'exploitation/logiciel.
	Hachage 0 de clé publique SGX LE : définit les octets à partir de 0 - 7 pour la valeur de hachage de la clé publique de l'enclave pour le lancement de SGX.
	Hachage 1 de clé publique SGX LE : définit les octets à partir de 8 - 15 pour la valeur de hachage de la clé publique de l'enclave pour le lancement de SGX.
	Hachage 2 de clé publique SGX LE : définit les octets à partir de 16 - 23 pour la valeur de hachage de la clé publique de l'enclave pour le lancement de SGX.
	Hachage 3 de clé publique SGX LE : définit les octets à partir de 24 - 31 pour la valeur de hachage de la clé publique de l'enclave pour le lancement de SGX.
Activation/désactivation de l'agent d'enregistrement MP automatique SGX	Cette option permet de désactiver l'enregistrement MP automatique SGX. L'agent d'enregistrement MP est chargé de l'enregistrement de la plate-forme.
Rétablir les paramètres SGX d'usine.	Cette option permet de rétablir les paramètres d'usine de l'option SGX. Par défaut, cette option est définie sur **Désactivé**.
Bouton d'alimentation	Vous permet d'activer ou de désactiver le bouton d'alimentation sur l'avant du système. Par défaut, cette option est définie sur **Enabled (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**. **REMARQUE :** Le système hôte ne se met pas sous tension tant qu'iDRAC Root of Trust (RoT) n'est pas terminé. La mise sous tension de l'hôte est alors retardée d'au moins 90 secondes après l'application d'une alimentation c.a.
Délai de restauration de l'alimentation secteur	Permet de définir au bout de combien de temps le système se met sous tension une fois qu'a été rétablie son alimentation secteur. Par défaut, l'option est réglée sur système. Par défaut, l'option est définie sur **Immédiatement**. Lorsque cette option est définie sur **Immédiatement**, il n'existe aucun délai avant la mise sous tension. Lorsque cette option est définie sur **Aléatoire**, il existe un délai aléatoire avant la mise sous tension. Lorsque cette option est définie sur **Défini par l'utilisateur**, le délai aléatoire avant la mise sous tension est défini manuellement.
Délai défini par l'utilisateur (60 s à 600 s)	Permet de régler le paramètre **Délai défini par l'utilisateur** lorsque l'option **Défini par l'utilisateur** pour **Délai de récupération de l'alimentation secteur** est sélectionnée. Le délai de reprise réel du CA doit ajouter le délai pour la racine de confiance (RoT) de l'iDRAC (environ 50 secondes).
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. Lorsque l'option est définie sur **contrôlé**, les variables UEFI sélectionnées

Tableau 5. Détails de l'écran Sécurité des systèmes (suite)

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>sont protégées dans l'environnement et de nouvelles entrées de démarrage UEFI sont obligées d'être à la fin de l'ordre de démarrage.</td></tr>
<tr><td>Interface de facilité de gestion intrabande</td><td>Lorsqu'il est défini sur Désactivé, ce paramètre cache le système Management Engine (ME), les appareils HECI et les appareils IPMI 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.</td></tr>
<tr><td>Migration de sécurité SMM</td><td>Cette option permet d'activer ou de désactiver les protections de la migration de la sécurité UEFI SMM. Il est activé pour la prise en charge de Windows 2022.</td></tr>
<tr><td>Secure Boot</td><td>Permet d'activer Secure Boot, où le BIOS authentifie chaque image de préamorçage à l'aide des certificats de la politique Secure Boot. Par défaut, la politique Secure Boot est définie sur Désactivé (par défaut).</td></tr>
<tr><td>Politique Secure Boot</td><td>Lorsque la politique 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 politique Secure Boot est définie sur Personnalisé, le BIOS utilise des clés et des certificats définis par l'utilisateur. Par défaut, la politique Secure Boot est définie sur Standard.</td></tr>
<tr><td>Mode Secure Boot</td><td>Configure la façon dont le BIOS utilise les objets de politique 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 User Mode, Mode d'audit, et mode déployé.
Tableau 6. Mode Secure Boot
<table>
<tr><th>Options</th><th>Descriptions</th></tr>
<tr><td>User Mode</td><td>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 système permet secteur incompatible lien logique entre les transitions entre les modes.</td></tr>
<tr><td>Mode d'audit</td><td>En Mode d'audit, PK n'est pas présent. Le BIOS n'authentifie pas la mise à jour programmatique des objets de stratégie et les transitions entre modes. Le BIOS effectue une vérification de signature sur les images de prédémarrage et consigne les résultats dans le tableau d'informations sur l'exécution. Il exécute toutefois les images, que leur vérification ait réussi ou échoué.
Mode d'audit est utile pour programmer un ensemble d'objets de politique.</td></tr>
<tr><td>Deployed Mode</td><td>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.</td></tr>
</table></td></tr>
<tr><td>Résumé de la politique Secure Boot</td><td>Spécifie la liste des certificats et des hachages qu'utilise Secure Boot pour authentifier des images.</td></tr>
<tr><td>Paramètres de la politique Secure Boot personnalisée</td><td>Configure la politique personnalisée Secure Boot. Pour activer cette option, définissez la politique Secure Boot sur option personnalisée. La liste ci-dessous décrit les différents paramètres de stratégie personnalisée Secure Boot disponibles :
• Clé de plateforme (PK) : Permet d'importer, d'exporter, de supprimer ou de restaurer la clé de plateforme (PK – Platform Key –).</td></tr>
</table>

Tableau 5. Détails de l'écran Sécurité des systèmes (suite)

Option	Description
	• **Base de données KEK (KEK)** : Permet d'importer, d'exporter, de supprimer ou de restaurer des entrées dans la base de données KEK (Key Exchange Key) • **Base de données des signatures autorisées (db)** : Permet d'importer, d'exporter, de supprimer ou de restaurer des entrées dans la base de données des signatures autorisées (db). • **Base de données des signatures non autorisées (dbx)** : Permet d'importer, d'exporter, de supprimer ou de restaurer des entrées dans la base de données des signatures non autorisées (dbx). • **Supprimer les entrées pour toutes les stratégies (PK, KEK, db et dbx)** : Permet de restaurer les entrées par défaut du fabricant du système dans les bases de données PK, KEK, db et dbx. Toutes les entrées importées seront supprimées. • **Exporter les valeurs de hachage des micrologiciels** : Permet d'exporter les valeurs des images de micrologiciels tiers (micrologiciel du contrôleur réseau, micrologiciel du contrôleur de stockage, etc.). ○ **Sélectionner une image de micrologiciel** : Fournit une liste des images de micrologiciels tiers que le système a tenté de charger au démarrage. Choisissez-en une, puis sélectionnez « Exporter » pour écrire sa valeur de hachage SHA-256 dans un fichier. ○ **Exporter l'entrée sélectionnée** : Écrit l'entrée de base de données sélectionnée dans un fichier.

4

Spécifications des blocs d'alimentation (PSU)

Le système PowerEdge T550 prend en charge jusqu'à deux blocs d'alimentation secteur :

Tableau 7. Spécifications des blocs d'alimentation (PSU)

Bloc d'alimentation	Classe	Dissipation thermique (maximale)	Fréquence	Tension	CA		CC	Courant
					Haute tension 200–240 V	Basse tension 100–120 V		
600 W en mode mixte	Platinum	2 250 BTU/h	50/60 Hz	100 à 240 V, sélection automatique	600 W	600 W	s.o.	7,1 A à 3,6 A
	s.o.	2 250 BTU/h	s.o.	240 V CC	s.o.	s.o.	600 W	2,9 A
800 W en mode mixte	Platinum	3 000 BTU/h	50/60 Hz	100 à 240 V, sélection automatique	800 W	800 W	s.o.	9,2 A à 4,7 A
	s.o.	3 000 BTU/h	s.o.	240 V CC	s.o.	s.o.	800 W	3,8 A
1 100 W CC	s.o.	4 265 BTU/h	s.o.	-48 VDC - -60 VDC	s.o.	s.o.	1 100 W	27 A
1 100 W en mode mixte	Titanium	4 125 BTU/hr	50/60 Hz	100 à 240 V	1 100 W	1 050 W	s.o.	12 A à 6,3 A
	s.o.	4 125 BTU/hr	s.o.	240 V CC	s.o.	s.o.	1 100 W	5,2 A
1 400 W en mode mixte	Platinum	5 250 BTU/h	50/60 Hz	100 à 240 V	1 400 W	1 050 W	s.o.	12 A à 8 A
	s.o.	5 250 BTU/h	s.o.	240 V CC	s.o.	s.o.	1 400 W	6,6 A
2 400 W en mode mixte	Platinum	9 000 BTU/h	50/60 Hz	100 à 240 V	2 400 W	1 400 W	s.o.	16 A à 13,5 A
	s.o.	9 000 BTU/h	s.o.	240 V CC	s.o.	s.o.	2 400 W	11,2 A
700 W en mode mixte	Titanium	2 625 BTU/hr	50/60 Hz	200-240 V CA	700 W	S/O	S/O	4,1 A
	S/O	2 625 BTU/hr	S/O	240 V CC	S/O	S/O	700 W	3,4 A
1 800 W en mode mixte	Titanium	6 000 BTU/hr	50/60 Hz	200-240 V CA	1 800 W	S/O	S/O	10 A
	S/O	6 000 BTU/h	S/O	240 V CC	S/O	S/O	1 800 W	8,2 A

REMARQUE : Ce système est également conçu pour se connecter aux systèmes d'alimentation informatiques avec une tension phase à phase ne dépassant pas 240 V.

REMARQUE : La dissipation thermique est calculée à partir de la puissance nominale du bloc d'alimentation.

REMARQUE : Lorsque vous sélectionnez ou mettez à niveau la configuration du système, vérifiez sa consommation électrique avec Dell Enterprise Infrastructure Planning Tool (disponible sur Dell.com/ESSA) pour assurer une utilisation optimale de l'alimentation.