Dell EMC PowerEdge R6525

Guide de référence du BIOS et de l'UEFI

Numéro de pièce détachée: E67S
Type réglementaire: E67S001
Août 2022
Rév. A08

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

Applications de gestion pré-système d'exploitation

Vous pouvez gérer les paramètres et fonctionnalités de base d'un système sans amorçage sur le système d'exploitation en utilisant le micrologiciel du système.

Options permettant de gérer les applications pré-système d'exploitation

Vous pouvez utiliser l'une des options suivantes pour gérer les applications pré-système d'exploitation :

- System Setup (Configuration du système)
- Dell Lifecycle Controller
- Boot Manager (Gestionnaire d'amorçage)
- Preboot Execution Environment (Environnement d'exécution de préamorçage, PXE)

Sujets :

Configuration du système

L'écran **Configuration du système** permet de configurer les paramètres du BIOS, les paramètres de l'iDRAC et les paramètres des appareils du système.

Vous pouvez accéder au menu de configuration du système via l'une des interfaces suivantes :

- Interface graphique : pour accéder au tableau de bord de l'iDRAC, cliquez sur **Configuration**, puis sur **Paramètres du BIOS**.
- Navigateur de texte : le navigateur est activé à l'aide de Redirection de la console.

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

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

Les détails de l'écran **Menu principal de la configuration du système** sont décrits ci-dessous :

Tableau 1. Menu principal de la configuration du système

Option	Description
BIOS du système	Permet de configurer les paramètres du BIOS.
Paramètres iDRAC	Permet de configurer les paramètres de l'iDRAC. L'utilitaire de configuration iDRAC est une interface permettant d'installer et de configurer les paramètres iDRAC utilisant l'UEFI. Vous pouvez activer ou désactiver de nombreux paramètres iDRAC à l'aide de l'utilitaire iDRAC Settings (Paramètres iDRAC). Pour plus d'informations sur cet utilitaire, consultez le document *Integrated Dell Remote Access Controller*

Tableau 1. Menu principal de la configuration du système (suite)

Option	Description
	User's Guide (Guide de l'utilisateur du contrôleur iDRAC) à l'adresse www.dell.com/poweredgemanuals.
Paramètres de l'appareil	Permet de configurer les paramètres des appareils tels que les contrôleurs de stockage ou les cartes réseau.

BIOS du système

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

Tableau 2. Description du BIOS du système

Option	Description
Informations sur le système	Spécifie les informations sur le système telles que le nom du modèle du système, la version du BIOS et le numéro de série.
Paramètres de mémoire	Spécifie les informations et les options relatives à la mémoire installée.
Paramètres du processeur	Spécifie les informations et les options relatives au processeur telles que la vitesse et la taille du cache.
Paramètres SATA	Spécifie les options permettant d'activer ou de désactiver le contrôleur et les ports SATA intégrés.
Paramètres NVMe	Spécifie les options permettant de modifier les paramètres réseau. Si le système contient les lecteurs NVMe que vous souhaitez configurer dans une baie RAID, vous devez définir ce champ et le champ **disque SATA intégré** dans le menu **Paramètres SATA** vers le mode **RAID**. Vous devrez peut-être également modifier les paramètres du **mode d'amorçagepour UEFI**. Sinon, vous devez définir ce champ sur le mode**Non RAID**.
Paramètres de démarrage	Permet d'afficher les options pour indiquer le mode d'amorçage (BIOS ou UEFI). Vous permet de modifier les paramètres de démarrage UEFI et BIOS.
Paramètres réseau	Spécifie les options pour gérer les paramètres réseau et protocoles de démarrage UEFI. Les paramètres réseau hérités sont gérés dans le menu **Paramètres de l'appareil**. **REMARQUE :** Les paramètres réseau ne sont pas pris en charge en mode d'amorçage du BIOS.
Périphériques intégrés	Spécifie les options permettant de gérer les ports et les contrôleurs d'appareils intégrés, ainsi que les fonctionnalités et options associées.
Communications série	Spécifie les options permettant de gérer les ports série, ainsi que les fonctionnalités et options associées.
Paramètres du profil du système	Spécifie les options permettant de modifier les paramètres de gestion de l'alimentation du processeur, la fréquence de la mémoire, etc.
Sécurité des systèmes	Permet d'afficher les options conçues pour configurer les paramètres de sécurité des systèmes, tels que le mot de passe du système, le mot de passe de la configuration, la sécurité TPM (Trusted Platform Module) et le mode Secure Boot UEFI. Permet également de gérer le bouton d'alimentation du système.
Contrôle du système d'exploitation redondant	Définit les informations du système d'exploitation redondant pour le contrôle du système d'exploitation redondant.
Paramètres divers	Spécifie les options permettant de modifier la date et l'heure du système,etc.

Informations sur le système

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

Tableau 3. Description des Informations système

Option	Description
Nom de modèle du système	Spécifie le nom du modèle du système.
Version du BIOS du système.	Spécifie la version du BIOS installée sur le système.
Numéro de série du système	Spécifie le numéro de série du système.
Fabricant du système.	Spécifie le nom du fabricant du système.
Coordonnées du fabricant du système.	Spécifie les coordonnées du fabricant du système.
Version CPLD du système	Spécifie la version actuelle du micrologiciel du circuit logique programmable complexe (CPLD) du système.
UEFI version de la conformité	Spécifie le niveau de conformité UEFI du micrologiciel système.
Version du protocole AGESA	Spécifie la version du code de référence du protocole AGESA.
Version du micrologiciel SMU	Spécifie la version du micrologiciel SMU.
Version du micrologiciel DXIO	Spécifie la version du micrologiciel DXIO.

Paramètres de mémoire

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

Tableau 4. Détails de l'écran Paramètres de la mémoire

Option	Description
Taille de la mémoire système	Spécifie la taille de la mémoire du système.
Type de mémoire système	Indique le type de la mémoire installée dans le système.
Vitesse de la mémoire système	Indique la vitesse de la mémoire système.
Tension de la mémoire système	Indique la tension de la mémoire système.
Mémoire vidéo	Indique la quantité de mémoire vidéo disponible.
Tests de la mémoire système	Indique si les tests de la mémoire système sont exécutés pendant l'amorçage du système. Les deux options disponibles sont **Activé** et **Désactivé**. Par défaut, cette option est définie sur **Désactivé**.
Délai d'actualisation de la DRAM	Si vous activez le **contrôleur de mémoire du processeur** pour retarder l'exécution des commandes **REFRESH**, vous pouvez améliorer les performances de certaines charges applicatives. En réduisant le délai, vous vous assurez que le contrôleur de mémoire exécute la commande **REFRESH**à intervalles réguliers. Pour les serveurs avec processeur Intel, ce paramètre affecte uniquement les systèmes configurés avec des modules DIMM qui utilisent des DRAM de 8 Go de densité. Par défaut, cette option est définie sur **Minimum**.
Mode de fonctionnement de la mémoire	Indique le mode de fonctionnement de la mémoire. L'option est disponible et définie par défaut sur **Mode Optimiseur**.
État actuel du mode de fonctionnement de la mémoire	Spécifie l'état actuel du mode de fonctionnement de la mémoire.

Tableau 4. Détails de l'écran Paramètres de la mémoire (suite)

Option	Description
Entrelacement de la mémoire	Active ou désactive l'option d'entrelacement de la mémoire. Les deux options disponibles sont **Auto** et **Désactivé**. Par défaut, cette option est définie sur **Auto**.
Journalisation des erreurs corrigibles	Active ou désactive la journalisation des erreurs corrigibles. Par défaut, cette option est définie sur **Activé**.
Réparation automatique des modules DIMM (réparation post-package) en cas d'erreur de mémoire non corrigible	Active ou désactive la réparation post-package (PPR) en cas d'erreur de mémoire non corrigible. Par défaut, cette option est définie sur **Activé**.

Paramètres du processeur

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

Tableau 5. Détails des paramètres du processeur

Option	Description
Processeur logique	Chaque cœur de processeur prend en charge jusqu'à deux processeurs logiques. Si cette option est définie sur **Activé**, le BIOS affiche tous les processeurs logiques. Si cette option est définie sur **Désactivé**, le BIOS n'affiche qu'un processeur logique par cœur. Par défaut, cette option est définie sur **Activé**.
Virtualization Technology	Active ou désactive la technologie de virtualisation pour le processeur. Par défaut, cette option est définie sur **Activé**.
Support IOMMU	Active ou désactive le support IOMMU. Il est nécessaire de créer le tableau ACPI IVRS. Par défaut, cette option est définie sur **Activé**.
Protection DMA du noyau	Lorsque cette option est définie sur Activé, à l'aide de l'IOMMU, le BIOS et le système d'exploitation vont activer l'option DMAP (Direct Memory Access Protection) pour les périphériques compatibles DMA. Activez la **prise en charge IOMMU** pour utiliser cette option. Par défaut, cette option est définie sur **Désactivé**. Lorsque cette option est définie sur Activé, à l'aide de la technologie de virtualisation, le BIOS et le système d'exploitation vont activer l'option DMAP (Direct Memory Access Protection) pour les périphériques compatibles DMA. Activez la technologie de virtualisation pour utiliser cette option.
Prélecteur du flux de matériel L1	Permet d'activer ou de désactiver le prélecteur du flux de matériel L1. Par défaut, cette option est définie sur **Activé**.
Prélecteur du flux de matériel L2	Permet d'activer ou de désactiver le prélecteur du flux de matériel L2. Par défaut, cette option est définie sur **Activé**.
Prélecteur de stride L1	Active ou désactive le prélecteur de stride L1. Par défaut, cette option est définie sur **Activé**, car elle optimise la charge applicative globale.
Prérécupération de zone géographique L1	Active ou désactive la prérécupération de zone géographique L1. Par défaut, cette option est définie sur **Activé**, car elle optimise la charge applicative globale.
Prélecteur haut/bas L2	Active ou désactive le prélecteur haut/bas L2. Par défaut, cette option est définie sur **Activé**, car elle optimise la charge applicative globale.
Énumération MADT Core	Spécifie l'énumération MADT Core. Par défaut, cette option est définie sur **Linéaire**.

Tableau 5. Détails des paramètres du processeur (suite)

Option	Description
Nœuds NUMA par socket	Spécifie le nombre de nœuds NUMA par socket. Par défaut, cette option est définie sur **1**.
CCX en tant que domaine NUMA	Permet d'activer ou de désactiver le CCX en tant que domaine NUMA. Par défaut, cette option est définie sur **Désactivé**.
Chiffrement de mémoire sécurisé (SME)	Active ou désactive les fonctions de chiffrement sécurisé AMD, telles que **SME** et **Secure Encrypted Virtualization (SEV)**. Cette option détermine également si d'autres fonctions de chiffrement sécurisé, telles que **TSME** et **SEV-SNP** peuvent être activées. Par défaut, cette option est définie sur **Désactivé**.
ASID SEV et non ES minimum	Détermine le nombre d'ID d'espace d'adressage disponible Secure Encrypted Virtualization ES et non ES Par défaut, cette option est définie sur **1**.
Pagination imbriquée sécurisée (SNP)	Active ou désactive **SEV-SNP**, un ensemble de protections de sécurité supplémentaires. Par défaut, cette option est définie sur **Désactivé**.
Couverture de la mémoire SNP	Cette option sélectionne le mode de fonctionnement de la mémoire de pagination imbriquée sécurisée (SNP) et de la table de mappage inverse (RMP). La RMP est utilisée pour garantir un mappage un à un entre les adresses physiques du système et les adresses physiques de l'invité.
Chiffrement transparent de la mémoire sécurisée (TSME)	Active ou désactive le chiffrement **TSME**. **TSME** est un chiffrement permanent de la mémoire qui ne nécessite pas de prise en charge du système d'exploitation ou de l'hyperviseur. Par défaut, cette option est définie sur **Désactivé**. ● Si le système d'exploitation prend en charge **SME**, n'activez pas ce champ. ● Si l'hyperviseur prend en charge **SEV**, n'activez pas ce champ. L'activation de **TSME** a une incidence sur les performances de la mémoire système.
Fonctionnalité REP MOVSB/URSB améliorée	Active ou désactive la prise en charge de REP MOVSB/URSB amélioré. Ce paramètre peut affecter les performances, en fonction de l'application exécutée sur le serveur. Par défaut, cette option est définie sur **Désactivé**. **REMARQUE :** Cette option est uniquement disponible pour le processeur AMD EPYC 7003.
Fast Short REP MOVSB	Active ou désactive la prise en charge de Fast Short REP MOVSB. Ce paramètre peut affecter les performances, en fonction de l'application exécutée sur le serveur. Par défaut, cette option est définie sur **Désactivé**. **REMARQUE :** Cette option est uniquement disponible pour le processeur AMD EPYC 7003.
Streaming REP-MOV/STOS	Permet d'activer ou de désactiver la prise en charge du streaming REP MOVISTOS. Ce paramètre peut affecter les performances, en fonction de l'application exécutée sur le serveur. Par défaut, cette option est définie sur **Désactivé**. **REMARQUE :** Cette option est uniquement disponible pour le processeur AMD EPYC 7003.
Puissance thermique configurable	Permet de reconfigurer les niveaux TDP (Thermal Design Power) du processeur en fonction des fonctionnalités de livraison d'alimentation et de puissance thermique du système. TDP fait référence à la puissance maximale de dissipation thermique par le

Tableau 5. Détails des paramètres du processeur (suite)

Option	Description
	système de refroidissement. Par défaut, cette option est définie sur **Maximum**. **REMARQUE :** Cette option n'est disponible que sur certaines SKU des processeurs et le nombre de niveaux alternatifs varie également.
Mode x2APIC	Permet d'activer ou de désactiver le mode x2APIC. Par défaut, cette option est définie sur **Activé**. **REMARQUE :** Pour la configuration à deux processeurs de 64 cœurs, le mode x2APIC n'est pas commutable si les 256 threads sont activés (paramètres du BIOS : tous les CCD, cœurs et processeurs logiques activés).
Nombre de CCD par processeur	Permet de contrôler le nombre de CCD activés dans chaque processeur. Par défaut, cette option est définie sur **Tous**.
Nombre de cœurs par CCD	Spécifie le nombre de cœurs par CCD. Par défaut, cette option est définie sur **Tous**.
Vitesse du cœur du processeur	Spécifie la fréquence maximale du cœur du processeur.
Processeur n	**REMARQUE :** Selon le nombre de processeurs, il peut y avoir jusqu'à n processeurs répertoriés. Les paramètres suivants sont indiqués pour chaque processeur installé dans le système :

Tableau 6. Détails du processeur n

Option	Description
Famille-Modèle-Version	Spécifie la famille, le modèle et la version du processeur tels que définis par AMD.
Marque	Spécifie le nom de marque.
Cache de niveau 2	Spécifie la taille de la mémoire cache L2.
Cache de niveau 3	Spécifie la taille de la mémoire cache L3.
Nombre de cœurs	Spécifie le nombre de cœurs par processeur.
Microcode	Spécifie la version du microcode du processeur.

Paramètres SATA

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

Tableau 7. Description des Paramètres SATA

Option	Description
Disque SATA intégré	Permet de définir l'option SATA intégré sur le mode **Désactivé**, **AHCI**, ou **RAID**. Par défaut, cette option est définie sur **Mode AHCI**. **REMARQUE :** 1. Vous devrez peut-être également modifier les paramètres du mode d'amorçagepour UEFI. Sinon, vous devez définir ce champ sur le mode Non RAID. 2. Aucune prise en charge des systèmes d'exploitation ESXi et Ubuntu en mode RAID.

Tableau 7. Description des Paramètres SATA (suite)

Option	Description
Gel du verrouillage de sécurité	Permet d'envoyer la commande **Gel du verrouillage de sécurité** aux dsiques SATA intégrés au cours de l'auto-test de démarrage (POST). Cette option est applicable uniquement pour le Mode AHCI. Par défaut, cette option est définie sur **Activé**.
Cache en écriture	Permet d'activer ou de désactiver la commande des disques SATA intégrés au cours du POST (auto-test de démarrage). Par défaut, cette option est définie sur **Désactivé**.
Port n	Spécifie le type de disque de l'appareil sélectionné. Pour le mode **AHCI** ou **RAID**, la prise en charge du BIOS est toujours activée. **Tableau 8. Port n** **Options** / **Descriptions** **Modèle** : Spécifie le modèle de lecteur du périphérique sélectionné. **Type de disque** : Spécifie le type du lecteur connecté au port SATA. **Capacité** : Spécifie la capacité totale du disque dur. Ce champ n'est pas défini pour les supports amovibles, tels que les lecteurs optiques.

Paramètres NVMe

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

Tableau 9. Détails des paramètres NVMe

Option	Description
Mode NVMe	Cette option définit le mode des disques NVMe. Si le système comporte des disques NVMe à configurer dans une baie RAID, vous devez définir ce champ et le champ SATA intégré sur mode RAID dans le menu Paramètres SATA. Vous devrez peut-être également modifier le paramètre Mode d'amorçage sur UEFI. Par défaut, cette option est définie sur **Mode non-RAID**.
Pilote NVMe du BIOS	Les disques NVMe qualifiés par Dell utilisent toujours le pilote UEFINVMe intégré à l'EROS Dell. Lorsque cette option est définie sur Tous les lecteurs, le pilote du BIOS est également utilisé avec tous les disques NVMe du système qui n'ont pas été qualifiés par Dell. Par défaut, cette option est définie sur **Disques qualifiés par Dell**. **REMARQUE :** Lorsque cette option est définie sur Tous les lecteurs et que des disques NVMe non qualifiés par Dell sont présents, vous disposez d'une configuration qui n'a pas été validée, ce qui peut entraîner un comportement inattendu.

Paramètres de démarrage

Vous pouvez utiliser l'écran **Boot Settings (Paramètres de démarrage)** pour régler le mode de démarrage sur **BIOS** ou UEFI **UEFI**. Il vous permet également de spécifier l'ordre de démarrage.

- **UEFI** : L'Unified Extensible Firmware Interface (UEFI) est une nouvelle interface entre les systèmes d'exploitation et le micrologiciel de la plate-forme.. L'interface se compose de tableaux de données avec des informations relatives à la plate-forme, des appels de service de démarrage et d'exécution qui sont disponibles pour le système d'exploitation et son chargeur. Les avantages suivants sont disponibles lorsque le **mode de démarrage** est réglé sur **UEFI** :
  - Prise en charge des partitions de disque de plus de 2 To.
  - Sécurité renforcée (par exemple, Secure Boot UEFI).
  - Temps d'amorçage plus rapide.

REMARQUE : Vous devez utiliser uniquement le mode d'amorçage UEFI pour démarrer à partir des lecteurs NVMe.

- **BIOS** : Le **mode d'amorçage du BIOS** est le mode d'amorçage hérité. Il est maintenu pour une compatibilité descendante.

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

Tableau 10. Description des Paramètres d'amorçage

Option	Description
Mode de démarrage	Permet de définir le mode d'amorçage du système. Si le système d'exploitation prend en charge l'UEFI, vous pouvez définir cette option sur UEFI. Le réglage de ce champ sur BIOS permet la compatibilité avec des systèmes d'exploitation non UEFI. Par défaut, cette option est définie sur **UEFI**. **PRÉCAUTION : changer le mode de démarrage peut empêcher le démarrage du système si le système d'exploitation n'a pas été installé selon le même mode de démarrage.** **REMARQUE :** Le fait de définir ce champ sur UEFI désactive le menu **Paramètres d'amorçage du BIOS**.
Relancer la séquence de démarrage	Active ou désactive la fonction **Réessayer la séquence de démarrage**. Si l'option est définie sur **Activé** et que le système n'arrive pas à démarrer, ce dernier réexécute la séquence de démarrage après 30 secondes. Par défaut, cette option est définie sur **Activé**.
Basculement de disque dur	Permet d'activer ou de désactiver le basculement de disque dur. Par défaut, cette option est définie sur **Désactivé**.
Amorçage USB générique	Active ou désactive l'espace réservé à l'amorçage USB générique. Par défaut, cette option est définie sur **Désactivé**.
Espace réservé du disque dur	Permet d'activer ou de désactiver l'espace réservé du disque dur. Par défaut, cette option est définie sur **Désactivé**.
Nettoyer l'ensemble des variables et commandes Sysprep.	Lorsque ce paramètre est défini sur **Aucun**, le BIOS ne fait rien. Lorsque ce paramètre est défini sur **Oui**, le BIOS supprime les variables de Sysprep #### et SysPrepOrder . Cette option est ponctuelle, elle est réinitialisée sur Aucun lors de la suppression des variables. Ce paramètre réseau est disponible uniquement en **mode de démarrage UEFI**. Par défaut, l'option est définie sur **Aucun**.
Paramètres de démarrage UEFI	Spécifie la séquence de démarrage UEFI. Active ou désactive les options d'amorçage du UEFI. **REMARQUE :** Cette option permet de contrôler la séquence de démarrage UEFI. La première option de la liste sera tentée en premier. **Tableau 11. Paramètres de démarrage UEFI** **Option** / **Description** **Séquence de démarrage UEFI** — Permet de modifier l'ordre des périphériques d'amorçage. **Activer/désactiver les options de démarrage** — Permet de sélectionner les appareils d'amorçage activés ou désactivés.

Choix du mode d'amorçage du système

Le programme de configuration du système vous permet de spécifier un des modes de démarrage suivants pour l'installation du système d'exploitation :

- Le mode d'amorçage UEFI (par défaut) est une interface d'amorçage 64 bits améliorée.

  Si vous avez configuré le système pour qu'il démarre en mode UEFI, il remplace le BIOS du système.

1. Dans le **Menu principal de configuration du système**, cliquez sur **Paramètres de démarrage** et sélectionnez **Mode de démarrage**.

2. Sélectionnez le mode d'amorçage UEFI souhaité pour démarrer le système.

   PRÉCAUTION : changer le mode de démarrage peut empêcher le démarrage du système si le système d'exploitation n'a pas été installé selon le même mode de démarrage.

3. Lorsque le système a démarré dans le mode d'amorçage spécifié, vous pouvez installer votre système d'exploitation depuis ce mode.

REMARQUE : Les systèmes d'exploitation doivent être compatibles avec l'UEFI afin d'être installés en mode d'amorçage UEFI. Les systèmes d'exploitation DOS et 32 bits ne prennent pas en charge l'UEFI et ne peuvent être installés qu'à partir du mode d'amorçage BIOS.

REMARQUE : Pour obtenir les dernières informations sur les systèmes d'exploitation pris en charge, rendez-vous sur www.dell.com/ossupport.

Modification de la séquence de démarrage

À propos de cette tâche

Vous devrez peut-être modifier l'ordre d'amorçage si vous souhaitez amorcer à partir d'une clé USB ou d'un lecteur optique. La procédure ci-dessous peut être différente si vous avez sélectionné **BIOS** comme **Mode d'amorçage**.

REMARQUE : La modification de la séquence de démarrage du disque est uniquement prise en charge en mode d'amorçage du BIOS.

Étapes

1. Dans l'écran **Menu principal de configuration du système**, cliquez sur **BIOS du système** > **Paramètres d'amorçage** > **Paramètres d'amorçage UEFI** > **Séquence de démarrage UEFI**.
2. Utilisez les touches fléchées pour sélectionner un périphérique d'amorçage, puis utilisez les touches + et - pour déplacer le périphérique vers le haut ou le bas dans la liste.
3. Cliquez sur **Exit (Quitter)**, puis sur **Yes (Oui)** pour enregistrer les paramètres en quittant.

   REMARQUE : Vous pouvez également activer ou désactiver les appareils de la séquence de démarrage selon vos besoins.

Paramètres réseau

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

REMARQUE : Pour plus d'informations sur les paramètres de performances du réseau Linux, voir le *Guide de réglage d'un réseau Linux® pour serveurs avec processeurs AMD EPYC™* sur AMD.com.

REMARQUE : Les paramètres réseau ne sont pas pris en charge en mode d'amorçage du BIOS.

Tableau 12. Description des Paramètres réseau

Option	Description
Paramètres PXE de l'UEFI	Permet de contrôler la configuration du périphérique PXE UEFI.
Appareil PXE n (n = 1 à 4)	Permet d'activer ou de désactiver l'appareil. Lorsque cette option est activée, une option de démarrage PXE en mode UEFI est créée pour l'appareil.
Paramètres Appareil PXE n (n = 1 à 4)	Permet de contrôler la configuration de l'appareil PXE.
Paramètres HTTP de l'UEFI	Permet de contrôler la configuration du périphérique HTTP UEFI.
Périphérique HTTP n (n = de 1 à 4)	Permet d'activer ou de désactiver l'appareil. Lorsque cette option est activée, une option de démarrage UEFI HTTP est créée pour l'appareil.
Paramètres du périphérique HTTP n (n = de 1 à 4)	Permet de contrôler la configuration de l'appareil HTTP.
Paramètres iSCSI UEFI	Permet de contrôler la configuration de l'appareil iSCSI.

Tableau 13. Description des Paramètres du périphérique PXE n

Option	Description
Interface	Détermine l'interface NIC utilisée pour ce périphérique PXE.
Protocole	Détermine le protocole utilisé pour ce périphérique PXE. Par défaut, cette option est définie sur **IPv4** ou **IPv6**. Par défaut, l'option est définie sur **IPv4**.
VLAN	Active le VLAN pour le périphérique PXE. Cette option est définie sur **Activer** ou **Désactiver**. Cette option est définie sur **Désactiver** par défaut.
ID du VLAN	Affiche l'ID du VLAN pour ce périphérique PXE
Priorité du VLAN	Détermine la priorité du VLAN pour ce périphérique PXE.

Tableau 14. Description des Paramètres du périphérique HTTP n

Option	Description
Interface	Détermine l'interface NIC utilisée pour ce périphérique HTTP.
Protocole	Détermine le protocole utilisé pour ce périphérique HTTP. Par défaut, cette option est définie sur **IPv4** ou **IPv6**. Par défaut, l'option est définie sur **IPv4**. Les options suivantes seront disponibles lorsque le protocole sera configuré sur Ipv6 : **Configuration automatique** : activation/désactivation de la configuration automatique IPv6 pour ce périphérique HTTP. **Adresse Ipv6** : adresse de monodiffusion IPv6 pour ce périphérique HTTP. **Longueur du préfixe** : longueur du préfixe IPv6 (0-128) pour ce périphérique HTTP.
VLAN	Active le VLAN pour le périphérique HTTP. Cette option est définie sur **Activer** ou **Désactiver**. Cette option est définie sur **Désactiver** par défaut.
ID du VLAN	Affiche l'ID du VLAN pour ce périphérique HTTP
Priorité du VLAN	Détermine la priorité du VLAN pour ce périphérique HTTP.
DHCP	Permet d'activer ou de désactiver le protocole DHCP pour cet périphérique HTTP. Par défaut, l'option est définie sur **Activer**.
Adresse IP	Détermine l'adresse IP du périphérique HTTP.
Masque de sous-réseau	Détermine le masque de sous-réseau du périphérique HTTP.
Passerelle	Détermine la passerelle du périphérique HTTP.
Informations DNS par protocole DHCP	Permet d'activer ou de désactiver les informations DNS par protocole DHCP. Par défaut, l'option est définie sur **Activer**.
DNS principal	Détermine l'adresse IP du serveur DNS primaire du périphérique HTTP.
DNS secondaire	Détermine l'adresse IP du serveur DNS secondaire du périphérique HTTP.
URI	Permet d'obtenir l'URI à partir du serveur DHCP s'il n'est pas spécifié.

Tableau 15. Description des Paramètres iSCSI UEFI

Option	Description
Nom de l'initiateur iSCSI	Spécifie le nom de l'initiateur iSCSI au format IQN.
Appareil1 iSCSI	Active ou désactive l'appareil iSCSI. Lorsque cette option est désactivée, une option de démarrage UEFI est créée automatiquement pour l'appareil iSCSI. Par défaut, cette option est définie sur **Désactivé**.
Paramètres d'Appareil1 iSCSI	Permet de contrôler la configuration de l'appareil iSCSI.

Tableau 16. Description des Paramètres iSCSI du périphérique 1

Option	Description
Connexion 1	Active ou désactive la connexion iSCSI. Cette option est définie sur **Désactiver** par défaut.
Connexion 2	Active ou désactive la connexion iSCSI. Cette option est définie sur **Désactiver** par défaut.
Paramètres de la connexion 1	Permet de contrôler la configuration de la connexion iSCSI.
Paramètres de la connexion 2	Permet de contrôler la configuration de la connexion iSCSI.
Ordre de connexion	Permet de contrôler la séquence de réalisation des connexions iSCSI.

Périphériques intégrés

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

Tableau 17. Détails de l'écran Périphériques intégrés

Option	Description
Ports USB accessibles à l'utilisateur	Configure les ports USB accessibles à l'utilisateur. La sélection de **Ports arrière activés uniquement** désactive les ports USB avant, la sélection de **Tous les ports désactivés** désactive tous les ports USB avant et arrière, et la sélection de **Tous les ports désactivés (Dynamique)** désactive tous les ports USB avant et arrière pendant le test POST. Par défaut, cette option est définie sur **Tous les ports activés**. Si les ports USB accessibles à l'utilisateur sont définis sur **Tous les ports désactivés (Dynamique)**, l'option **Activer les ports avant uniquement** est activée. • **Activer les ports avant uniquement** : active ou désactive les ports USB avant lors de l'exécution du système d'exploitation. Le clavier et la souris USB fonctionnent toujours sur certains ports USB pendant le processus de démarrage, en fonction de la sélection. Une fois le processus d'amorçage terminé, les ports USB sont activés ou désactivés en fonction de la configuration.
Port USB interne	Active ou désactive l'option **Port USB interne**. Cette option est définie sur **Activé** ou **Désactivé**. Par défaut, cette option est définie sur **Activé**.
Port USB iDRAC Direct	Le port USB iDRAC Direct est géré par l'iDRAC exclusivement sans visibilité sur l'hôte. Cette option est définie sur **Activé** ou **Désactivé**. Lorsqu'elle est définie sur **Désactivé**, iDRAC ne détecte aucun périphérique USB installé dans ce port. Par défaut, cette option est définie sur **Activé**.
Contrôleur RAID intégré	Permet d'activer ou de contrôleur RAID intégré. Par défaut, cette option est définie sur **Activé**.
Cartes NIC1 et NIC2 intégrées	Active ou désactive l'option **Cartes NIC1 et NIC2 intégrées**. Si cette option est définie sur **Désactivé (SE)**, la carte NIC peut toujours être disponible pour l'accès réseau partagé par le contrôleur de gestion intégré. Configurez l'option **Cartes NIC1 et NIC2 intégrées** à l'aide des utilitaires de gestion de carte réseau du système.
Contrôleur vidéo intégré	Active ou désactive l'utilisation du contrôleur vidéo intégré comme affichage principal. Lorsque l'option est définie sur **Activé**, le contrôleur vidéo intégré sera l'affichage principal, même si des cartes graphiques supplémentaires sont installées. Lorsque l'option est définie sur **Désactivé**, une carte graphique supplémentaire sera utilisée comme affichage principal. Au cours de l'auto-test de démarrage et dans l'environnement de pré-amorçage, le BIOS s'affiche sur la carte vidéo supplémentaire ainsi que sur le contrôleur vidéo intégré. Le contrôleur vidéo intégré sera désactivé juste avant le démarrage du système d'exploitation. Par défaut, cette option est définie sur **Activé**.

Tableau 17. Détails de l'écran Périphériques intégrés (suite)

Option	Description
	REMARQUE : Lorsqu'il y a plusieurs cartes graphiques supplémentaires installées sur le système, la première carte découverte pendant l'énumération PCI est sélectionnée comme source vidéo principale. Il est possible que vous ayez à réorganiser les cartes dans les logements pour identifier la carte principale.
État actuel du contrôleur vidéo intégré	Indique l'état actuel du contrôleur vidéo intégré. L'option **État actuel du contrôleur vidéo intégré** est un champ en lecture seule. Si le contrôleur vidéo intégré est le seul moyen d'affichage dans le système (autrement dit, aucune carte graphique supplémentaire n'est installée), alors le contrôleur vidéo intégré est automatiquement utilisé comme affichage principal, même si le paramètre **Contrôleur vidéo intégré** est défini sur **Désactivé**.
Fréquence LCLK pour la racine complexe 0x00	Définit la fréquence LCLK de l'adresse de bus 0x00.
Fréquence LCLK pour la racine complexe 0x20	Définit la fréquence LCLK de l'adresse de bus 0x20.
Fréquence LCLK pour la racine complexe 0x40	Définit la fréquence LCLK de l'adresse de bus 0x40.
Fréquence LCLK pour la racine complexe 0x60	Définit la fréquence LCLK de l'adresse de bus 0x60.
Fréquence LCLK pour la racine complexe 0x80	Définit la fréquence LCLK de l'adresse de bus 0x80.
Fréquence LCLK pour la racine complexe 0xA0	Définit la fréquence LCLK de l'adresse de bus 0xA0.
Fréquence LCLK pour la racine complexe 0xC0	Définit la fréquence LCLK de l'adresse de bus 0xC0.
Fréquence LCLK pour la racine complexe 0xE0	Définit la fréquence LCLK de l'adresse de bus 0xE0.
Préférence Bus d'E/S PCIe	Si cette option est définie sur **Activé**, vous pouvez indiquer l'adresse du bus, de l'appareil ou de la fonction (au format décimal) pour choisir l'appareil d'E/S favori. Par défaut, cette option est définie sur **Désactivé**.
Préférence E/S avancées	Si cette option est définie sur **Activé**, la vitesse LCLK pour la racine complexe où la préférence E/S est activée est automatiquement définie sur 600 MHz (efficace : 593 MHz).
Activation des périphériques SR-IOV avec la commande globale	Permet d'activer ou de désactiver la configuration du BIOS des périphériques SR-IOV (Single Root I/O Virtualization). Par défaut, cette option est définie sur **Désactivé**.
Port de la carte SD interne	Permet d'activer ou de désactiver le port de carte SD interne du module SD interne double (IDSDM). Par défaut, cette option est définie sur **Activé**.
Redondance de la carte SD interne	Configure le mode de redondance du module IDSDM. Lorsque l'option est réglée sur le mode **Miroir**, les données sont écrites sur les deux cartes SD. En cas de défaillance de l'une des cartes et de remplacement de la carte défaillante, les données de la carte active sont copiées sur la carte hors ligne au cours de l'amorçage du système. Lorsque la redondance de la carte SD interne est défini sur **Désactivé**, seule la carte SD principale est visible sous le système d'exploitation. Par défaut, cette option est définie sur **Miroir**.
Carte SD principale interne	Par défaut, la carte SD principale est sélectionnée comme carte SD 1. Si la carte SD 1 n'est pas présente, le contrôleur doit sélectionner la carte SD 2 en tant que carte SD principale. Par défaut, cette option est définie sur **Carte SD 1**.
Minuteur de surveillance du système d'exploitation	Si le système ne répond plus, ce minuteur de surveillance aide à la restauration du système d'exploitation. Lorsque cette option est définie sur **Activé**, le système

Tableau 17. Détails de l'écran Périphériques intégrés (suite)

Option	Description
	d'exploitation initialise le minuteur. Lorsque cette option est définie sur **Désactivé** (valeur par défaut), le minuteur n'a aucun effet sur le système.
Limite d'E/S du mappage mémoire	Contrôle le mappage du MMIO. L'option **1 To** est conçue pour les systèmes d'exploitation spécifiques qui ne peuvent pas prendre en charge les MMIO au-delà de 1 To. Par défaut, cette option est définie sur **8 To**. L'option par défaut est l'adresse maximale que le système prend en charge. Elle est recommandée dans la plupart des cas.
Désactivation des logements	Permet d'activer ou de désactiver les logements PCIe disponibles sur le système. La fonctionnalité Désactivation des logements contrôle la configuration des cartes PCIe installées dans un logement spécifique. Les logements doivent être désactivés seulement lorsque la carte périphérique installée empêche l'amorçage dans le système d'exploitation ou lorsqu'elle cause des délais lors du démarrage du système. Si le logement est désactivé, l'option ROM et les pilotes UEFI sont aussi désactivés. Seuls les logements présents dans le système sont contrôlables. **Logement n** : active, désactive, ou désactive uniquement le pilote de démarrage pour le logement PCIe n. Par défaut, cette option est définie sur **Activé**.
Bifurcation des logements	**Paramètres de fractionnement de détection de logement** permet le **Fractionnement par défaut de la plate-forme** et le **Contrôle manuel des fractionnements**. La valeur par défaut est définie sur **Fractionnement par défaut de la plate-forme**. Le champ Fractionnement des logements est accessible lorsqu'il est défini sur **Contrôle manuel des fractionnements** et est grisé lorsqu'il est défini sur **Fractionnement par défaut de la plate-forme**.

Communications série

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

REMARQUE : Le port série est facultatif (en option) pour le système PowerEdge R6525. La communication série (en option) n'est applicable que si le port série COM est installé dans le système.

Tableau 18. Détails de l'écran Communications série

Option	Description
Communications série	Désactive les périphériques de communication série (périphérique série 1 et périphérique série 2) dans le BIOS. La redirection de la console BIOS peut également être activée et l'adresse du port peut être indiquée. Par défaut, l'option est définie sur **Auto** .
Adresse du port série	Vous permet de définir l'adresse de port des périphériques série. Par défaut, cette option est définie sur **Périphérique série 1=COM2, Périphérique série 2=COM1**. **REMARQUE :** Vous ne pouvez utiliser que le périphérique série 2 pour la fonctionnalité SOL (Serial Over LAN, série sur réseau local). Pour utiliser la redirection de console par SOL, configurez la même adresse de port pour la redirection de console et le périphérique série. **REMARQUE :** Chaque fois que le système s'amorce, le BIOS synchronise le paramètre MUX série enregistré dans l'iDRAC. Le paramètre MUX série peut être modifié séparément dans l'iDRAC. Parfois le chargement des paramètres BIOS par défaut dans l'utilitaire de configuration du BIOS ne rétablit pas la valeur par défaut du paramètre MUX série (dispositif série 1).
Connecteur série externe	Permet d'associer le connecteur série externe au **Périphérique série 1**, **Périphérique série 2** ou **Périphérique d'accès à distance** à l'aide de cette option. Par défaut, cette option est définie sur **Périphérique série 1**.

Tableau 18. Détails de l'écran Communications série (suite)

Option	Description
	REMARQUE : Seul le périphérique série 2 peut être utilisé pour la connectivité SOL (Serial Over LAN). Pour utiliser la redirection de console par SOL, configurez la même adresse de port pour la redirection de console et le périphérique série. **REMARQUE :** Chaque fois que le système démarre, le BIOS synchronise le paramètre MUX série enregistré dans l'iDRAC. Le paramètre MUX série peut être modifié séparément dans l'iDRAC. Le chargement des paramètres par défaut du BIOS dans l'utilitaire de configuration du BIOS ne peut pas toujours faire revenir ce paramètre à celui par défaut du périphérique série 1.
Débit en bauds de la sécurité intégrée	Spécifie le débit en bauds de la sécurité intégrée pour la redirection de console. Le BIOS tente de déterminer le débit en bauds automatiquement. Ce débit est utilisé uniquement si la tentative échoue, et la valeur ne doit pas être modifiée. Par défaut, cette option est définie sur **115200**.
Type de terminal distant	Permet de définir le type de terminal de console distant. Par défaut, cette option est définie sur **VT100/VT220**.
Redirection de console après démarrage	Permet d'activer ou de désactiver la redirection de la console du BIOS lorsque le système d'exploitation est chargé. Par défaut, cette option est définie sur **Activé**.

Paramètres du profil du système

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

Tableau 19. Description des Paramètres du profil système

Option	Description
Profil système	Permet de définir le profil du système. Si vous définissez l'option **Profil du système** sur un mode autre que Personnalisé, le BIOS définit automatiquement le reste des options. Vous ne pouvez que modifier le reste des options si le mode est défini sur **Personnalisé**. Par défaut, cette option est définie sur **Performance par watt (SE).** Les autres options comprennent **Performances** et **Personnalisé**. **REMARQUE :** Tous les paramètres dans l'écran du profil système sont uniquement disponibles lorsque le **profil du système** est défini sur **Personnalisé**.
Gestion de l'alimentation du processeur	Permet de définir la gestion de l'alimentation du processeur. Par défaut, cette option est définie sur **DBPM du SE**. Une autre option est **Performances maximales**.
Fréquence de la mémoire	Permet de définir la fréquence de la mémoire système. Vous pouvez sélectionner **Performances maximales** ou une vitesse spécifique. Par défaut, cette option est définie sur **Surveillance anticipée**.
Turbo Boost	Permet d'activer ou de désactiver le processeur pour faire fonctionner le mode Turbo Boost. Par défaut, cette option est définie sur **Activé**.
États C	Active ou désactive le fonctionnement du processeur dans tous les états d'alimentation disponibles. La fonctionnalité États C permet au processeur d'entrer dans un état d'alimentation inférieur lorsqu'il est inactif. Lorsque cette option est définie sur **Activé** (contrôle par le système d'exploitation) ou sur **Autonome** (contrôle par le matériel pris en charge), le processeur peut fonctionner dans tous les États d'alimentation disponibles pour économiser l'énergie ; cependant, cela peut augmenter la latence de la mémoire et la gigue de fréquence. Par défaut, cette option est définie sur **Activé**.
Écrire des données CRC	Lorsque cette option est définie sur **Activé**, les problèmes du bus de données DDR4 sont détectés et corrigés lors des opérations « write ». Deux cycles supplémentaires sont requis pour la génération de bits CRC qui affecte les performances. Option en lecture seule, sauf si le paramètre Profil système est défini sur **Personnalisé**. Par défaut, cette option est définie sur **Désactivé**.

Tableau 19. Description des Paramètres du profil système (suite)

Option	Description
Révision cohérente de la mémoire	Permet de définir le mode de vérification et de correction d'erreur de la mémoire. Par défaut, cette option est définie sur **Standard**.
Taux d'actualisation de la mémoire	Définit le taux d'actualisation de la mémoire à 1x ou 2x. Par défaut, cette option est définie sur **1x**.
Gestion de l'alimentation de la liaison PCI ASPM L1	Active ou désactive la gestion de l'alimentation de liaison PCI ASPM L1. Par défaut, cette option est définie sur **Activé**.
Curseur de déterminisme	Permet de définir le déterminisme du système sur **Déterminisme par alimentation** ou **Déterminisme par performances**. Par défaut, cette option est définie sur **Déterminisme par alimentation**.
Mode Optimisation de l'efficacité	Le mode Optimisation de l'efficacité permet d'optimiser les performances par watt en optant pour la réduction opportuniste de la fréquence et de l'alimentation. Permet d'activer ou de désactiver le mode Optimisation de l'efficacité.
Désactivation de l'optimisation des performances d'algorithme (ApbDis)	Active ou désactive l'option de désactivation de l'optimisation des performances d'algorithme (ApbDis). Par défaut, cette option est définie sur **Désactivé**.
Vitesse max. XGMI	Ce champ indique la vitesse maximale XGMI du processeur.
Gestion de la largeur de liaison dynamique (DLWM)	Réduit la largeur de liaison xGMI entre les sockets x16 à x8 (valeur par défaut), lorsqu'aucun trafic n'est détecté sur la liaison. Par défaut, cette option est définie sur **Non forcée**.

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 20. 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**.

Tableau 21. Informations de sécurité du module TPM 1.2

Option	Description
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 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**. 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	Vous permet de modifier l'état opérationnel du module TPM. Cette option a la valeur **Aucune modification** par défaut.

Tableau 21. Informations de sécurité du module TPM 1.2 (suite)

Option	Description
TPM Firmware	Indique la version du firmware du TPM.
TPM Status	Spécifie l'état du module TPM.
TPM Command	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**.

Tableau 22. Informations de sécurité du module TPM 2.0

Option	Description
Informations TPM	Vous permet de modifier l'état opérationnel du module TPM. Cette option a la valeur **Aucune modification** par défaut.
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	Spécifie les détails des paramètres TPM avancés.

Tableau 23. Détails de l'écran Sécurité des systèmes

Option	Description
Fonctionnalité AmD DTRM (Dynamic Root of Trust Measurement)	Activer/désactiver la fonctionnalité AMD DRTM (Dynamic Root of Trust Measurement) Pour activer la fonctionnalité AMD DRTM, les configurations ci-dessous doivent être activées : 1. TPM2.0 doit être activé et l'algorithme de hachage doit être défini sur SHA256. 2. TSME (Transparent SME) doit être activé. 3. DMAP (Direct Memory Access Protection) doit être activée.
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 **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	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**.
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.
UEFI Variable Access	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'elle est définie 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.
Secure Boot	Permet d'activer l'Amorçage sécurisé, où le BIOS authentifie chaque image de préamorçage à l'aide des certificats de la stratégie d'amorçage sécurisé. Par défaut, la stratégie d'amorçage sécurisé est définie sur **Désactivé** (par défaut).
Politique d'amorçage sécurisé	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 d'amorçage sécurisé est définie sur **Personnalisé**, le BIOS utilise des clés et des

Tableau 23. Détails de l'écran Sécurité des systèmes (suite)

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>certificats définis par l'utilisateur. Par défaut, la stratégie d'amorçage sécurisé est définie sur Standard.</td></tr>
<tr><td>Mode d'amorçage sécurisé</td><td>Configure la façon dont le BIOS utilise la politique de démarrage sécurisé objets (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 24. Mode d'amorçage sécurisé
<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>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>
<tr><td>Audit Mode</td><td>En mode d'audit, PK n'est présente. Le BIOS n'authentifie pas mises à jour programmé pour les objets de politique, et les transitions entre les 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>
</table></td></tr>
<tr><td>Résumé de la stratégie d'amorçage sécurisé</td><td>Spécifie la liste des certificats et des hachages qu'utilise l'amorçage sécurisé pour authentifier des images.</td></tr>
<tr><td>Paramètres de la politique personnalisée d'amorçage sécurisé</td><td>Configure la stratégie personnalisée d'amorçage sécurisé. Pour activer cette option, définissez la politique de démarrage sécurisé sur option personnalisée.</td></tr>
</table>

Création d'un mot de passe système et de configuration

Prérequis

Assurez-vous que le cavalier de mot de passe est activée. Le cavalier de mot de passe active ou désactive les fonctions de mot de passe pour le système et la configuration. Pour plus d'informations, voir la section Paramétrage des cavaliers de la carte Système.

REMARQUE : Si le paramètre du cavalier du mot de passe est désactivé, le mot de passe du système et le mot de passe de configuration existants sont supprimés et vous n'avez pas besoin de fournir un mot de passe du système pour ouvrir une session.

Étapes

1. Pour accéder à la Configuration du système, appuyez sur la touche F2 immédiatement après le démarrage ou le redémarrage de votre système.
2. Dans l'écran **System Setup Main Menu (Menu principal de configuration du système)**, cliquez sur **System BIOS (BIOS du système)** > **System Security (Sécurité du système)**.
3. Dans l'écran **System Security (Sécurité du système)**, vérifiez que **Password Status (État du mot de passe)** est **Unlocked (Déverrouillé)**.
4. Dans le champ **Mot de passe du système**, saisissez votre mot de passe système, puis appuyez sur Entrée ou Tabulation.

   Suivez les instructions pour définir le mot de passe système :
   - Un mot de passe peut contenir jusqu'à 32 caractères.

Un message vous invite à ressaisir le mot de passe du système.

5. Entrez à nouveau le mot de passe du système, puis cliquez sur **OK**.
6. Dans le champ **Setup Password (configurer le mot de passe)**, saisissez votre mot de passe système, puis appuyez sur Entrée ou Tabulation.
   Un message vous invite à ressaisir le mot de passe de configuration.
7. Entrez à nouveau le mot de passe, puis cliquez sur **OK**.
8. Appuyez sur Échap pour revenir à l'écran BIOS du Système. Appuyez de nouveau sur Échap.
   Un message vous invite à enregistrer les modifications.

   REMARQUE : La protection par mot de passe ne prend effet que lorsque vous redémarrez le système.

Utilisation de votre mot de passe système pour sécuriser le système

À propos de cette tâche

Si vous avez attribué un mot de passe de configuration, le système l'accepte également comme mot de passe système alternatif.

Étapes

1. Allumez ou redémarrez le système.
2. Saisissez le mot de passe système, puis appuyez sur la touche Entrée.

Étapes suivantes

Si **État du mot de passe** est défini sur **Verrouillé**, saisissez le mot de passe système, puis appuyez sur Entrée lorsque le système vous invite au redémarrage.

REMARQUE : Si un mot de passe système incorrect est saisi, le système affiche un message et vous invite à saisir à nouveau votre mot de passe. Vous disposez de trois tentatives pour saisir le mot de passe correct. Après une troisième tentative infructueuse, le système affiche un message d'erreur indiquant que le système s'est arrêté et qu'il doit être éteint. Même après l'arrêt et le redémarrage du système, le message d'erreur continue à s'afficher tant que vous n'avez pas entré le mot de passe approprié.

Suppression ou modification du mot de passe d'système et de configuration

Prérequis

REMARQUE : Vous ne pouvez pas supprimer ou modifier un mot de passe d'système ou de configuration existant si le champ **Password Status** (État du mot de passe) est défini sur **Locked** (Verrouillé).

Étapes

1. Pour accéder à la configuration du système, appuyez sur la touche F2 immédiatement après le démarrage ou le redémarrage de l'système.
2. Dans l'écran **Menu principal de configuration du système**, cliquez sur **BIOS du système** > **Sécurité du système**.
3. Dans l'écran **System Security (Sécurité du système)**, vérifiez que le **Password Status (État du mot de passe)** est défini sur **Unlocked (Déverrouillé)**.
4. Dans le champ **System Password** (Mot de passe du système), modifiez ou supprimez le mot de passe d'système existant, puis appuyez sur la touche Entrée ou sur la touche Tab.
5. Dans le champ **Setup Password (Mot de passe de la configuration)**, modifiez ou supprimez le mot de passe existant, puis appuyez sur la touche Entrée ou sur la touche Tab.

   Si vous modifiez le mot de passe de l'système et de configuration, un message vous invite à saisir à nouveau le nouveau mot de passe. Si vous supprimez le mot de passe de l'système et de configuration, un message vous invite à confirmer la suppression.
6. Appuyez sur Échap pour revenir à l'écran **BIOS du système**. Appuyez de nouveau sur Échap pour faire apparaître une invite d'enregistrement des modifications.
7. Sélectionnez **Setup Password (Mot de passe de configuration)**, modifiez ou supprimez le mot de passe de configuration existant et appuyez sur Entrée ou sur Tab.

REMARQUE : Si vous modifiez le mot de passe du système et/ou de configuration, un message vous invite à ressaisir le nouveau mot de passe. Si vous supprimez le mot de passe du système et/ou de configuration, un message vous invite à confirmer la suppression.

Utilisation avec un mot de passe de configuration activé

Si l'option **Setup Password (Configuration du mot de passe)** est définie sur **Enabled (Activé)**, saisissez le mot de passe de configuration correct avant de modifier les options de configuration du système.

Si vous ne saisissez pas le mot de passe correct au bout de trois tentatives, le système affiche le message suivant :

```
Invalid Password! Number of unsuccessful password attempts: <x> System Halted! Must power
down.
```

```
Password Invalid. Number of unsuccessful password attempts: <x> Maximum number of password
attempts exceeded.System halted.
```

Même après l'arrêt et le redémarrage du système, le message d'erreur reste affiché tant que vous n'avez pas saisi le bon mot de passe. Les options suivantes sont des exceptions :

- Si l'option **System Password (Mot de passe du système)** n'est ni définie sur **Enabled (Activé)** ni verrouillée via l'option **Password Status (État du mot de passe)**, vous pouvez attribuer un mot de passe au système. Pour plus d'informations, reportez-vous à la section Paramètres de sécurité du Système.
- Vous ne pouvez ni désactiver ni modifier un mot de passe système existant.

REMARQUE : Il est possible de combiner l'utilisation des options Password Status (État du mot de passe) et Setup Password (Mot de passe de configuration) pour empêcher toute modification non autorisée du mot de passe système.

Contrôle du système d'exploitation redondant

Pour afficher l'écran **Contrôle du système d'exploitation redondant**, mettez le système sous tension, appuyez sur la touche F2, puis cliquez sur **Menu principal de configuration du système** > **BIOS du système** > **Contrôle du système d'exploitation redondant**.

Tableau 25. Détails de l'écran Contrôle du système d'exploitation redondant

Option	Description
Emplacement du système d'exploitation redondant	Vous permet de sélectionner un disque de sauvegarde depuis les périphériques suivants : • **Aucun** • **IDSDM** • **Mode Ports SATA en mode AHCI** • **Cartes PCIe BOSS (disques M.2 internes)** • • **USB interne** **REMARQUE :** Les configurations RAID et les cartes NVMe ne sont pas incluses, car le BIOS ne peut pas faire chaque disque de ces configurations.
État du système d'exploitation redondant	**REMARQUE :** Cette option est désactivée si l'option **Emplacement du système d'exploitation redondant** est définie sur **Aucun**. Lorsqu'elle est définie sur **Visible**, le disque de sauvegarde est visible pour la liste de démarrage et le système d'exploitation. Lorsqu'elle est définie sur **Hidden** (Masqué), le disque de sauvegarde est désactivé et n'est pas visible pour la liste de démarrage et le système d'exploitation. Par défaut, l'option est définie sur **Visible**. **REMARQUE :** Le BIOS désactive le périphérique au niveau du matériel, de sorte qu'il ne soit pas accessible par le système d'exploitation.
Démarrage d'OS redondant	**REMARQUE :** Cette option est désactivée si l'option **Emplacement du système d'exploitation redondant** est définie sur **Aucun** ou si l'option **État du système d'exploitation redondant** est définie sur **Masqué**.

Tableau 25. Détails de l'écran Contrôle du système d'exploitation redondant (suite)

Option	Description
	Lorsque la valeur est définie sur **Activé**, le BIOS démarre sur l'appareil spécifié dans l'**Emplacement de SE redondant**. Lorsqu'elle est définie sur **Désactivé**, le BIOS conserve les paramètres de la liste de démarrage actuelle. Par défaut, cette option est définie sur **Activé**.

Paramètres divers

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

Tableau 26. Description des Paramètres divers

Option	Description
Heure système	Permet de régler l'heure sur le système.
Date du système	Permet de régler la date sur le système.
Asset Tag (Numéro d'inventaire)	Indique le numéro d'inventaire et permet de le modifier à des fins de sécurité et de suivi.
Touche Verr Num	Vous permet de définir si le système démarre avec la fonction Verr Num activée ou désactivée. Par défaut, cette option est définie sur **Activé**. **REMARQUE :** Cette option ne s'applique pas aux claviers à 84 touches.
Invite F1/F2 en cas d'erreur	Permet d'activer ou de désactiver l'invite F1/F2 en cas d'erreur. Par défaut, cette option est définie sur **Activé**. L'invite F1/F2 inclut également les erreurs liées au clavier.
Charger l'option ROM vidéo héritée	Permet d'activer ou de désactiver le chargement des options vidéo conventionnelles avec la mémoire en lecture seule. Par défaut, cette option est définie sur **Désactivé**.
Accès au BIOS Dell Wyse P25/P45	Active ou désactive l'accès au BIOS Dell Wyse P25/P45. Par défaut, cette option est définie sur **Activé**.
Power Cycle Request (Demande cycle de marche/arrêt)	Active ou désactive la demande de cycle de marche/arrêt. Par défaut, l'option est définie sur **Aucun**.

Utilitaire de configuration iDRAC

L'utilitaire de configuration iDRAC est une interface permettant d'installer et de configurer les paramètres iDRAC en utilisant l'UEFI. Vous pouvez activer ou désactiver de nombreux paramètres iDRAC à l'aide de l'utilitaire iDRAC Settings (Paramètres iDRAC).

REMARQUE : L'accès à certaines fonctions de l'utilitaire Paramètres iDRAC exige une mise à niveau vers la licence iDRAC Enterprise.

Pour plus d'informations sur l'utilisation de l'iDRAC, voir le *Guide de l'utilisateur du contrôleur iDRAC* sur https://www.dell.com/idracmanuals.

Device Settings (Paramètres du périphérique)

L'option **Paramètres du périphérique** vous permet de configurer les paramètres de périphériques tels que les contrôleurs de stockage ou les cartes réseau.

Dell Lifecycle Controller

Dell Lifecycle Controller (LC) offre une gestion avancée des systèmes intégrés dont les formats de déploiement du système, sa configuration, sa mise à jour, sa maintenance, et ses diagnostics. LC est fourni en tant que composant du système hors-bande de l'iDRAC et solution Dell intégrées du système UEFI (Unified Extensible Firmware Interface) d'applications.

Gestion intégrée du système

Le Dell Lifecycle Controller offre une gestion avancée des systèmes intégrés tout au long du cycle de vie du système. Le Dell Lifecycle Controller est démarré pendant la séquence de démarrage et fonctionne indépendamment du système d'exploitation.

REMARQUE : Certaines configurations de plateforme peuvent ne pas prendre en charge l'ensemble des fonctionnalités du Lifecycle Controller.

Pour plus d'informations sur la configuration du Dell Lifecycle Controller, la configuration du matériel et du micrologiciel, et le déploiement du système d'exploitation, voir la documentation relative au Dell Lifecycle Controller sur https://www.dell.com/idracmanuals.

Boot Manager (Gestionnaire d'amorçage)

L'option **Gestionnaire d'amorçage** permet de sélectionner les options d'amorçage et les utilitaires de diagnostic.

Pour accéder au **Gestionnaire d'amorçage**, mettez le système sous tension, puis appuyez sur la touche F11.

Tableau 27. Options du Gestionnaire d'amorçage

Option	Description
Continue Normal Boot (Poursuivre le démarrage normal)	Le système tente d'effectuer successivement l'amorçage sur différents périphériques en commençant par le premier dans l'ordre d'amorçage. En cas d'échec de l'amorçage, le système passe au périphérique suivant dans l'ordre d'amorçage jusqu'à ce que le démarrage réussisse ou qu'aucune autre option ne soit disponible.
Menu One-shot Boot (Amorçage unique)	Vous permet d'accéder au menu d'amorçage, dans lequel vous pouvez sélectionner un périphérique d'amorçage unique à partir duquel démarrer.
Launch System Setup (Démarrer la configuration du système)	Permet d'accéder au programme de configuration du système.
Launch Lifecycle Controller	Permet de quitter le gestionnaire d'amorçage et appelle le programme Dell Lifecycle Controller.
System Utilities (Utilitaires du système)	Permet de lancer les éléments du menu Utilitaires système tels que Lancer les diagnostics, Explorateur de fichier de mise à jour du BIOS, Réamorçage du système.

Démarrage PXE

Vous pouvez utiliser l'option PXE (environnement d'exécution préamorçage) pour amorcer et configurer les systèmes en réseau à distance.

Pour accéder à l'option **Démarrage PXE**, démarrez le système, puis appuyez sur F12 pendant la phase POST au lieu d'utiliser la séquence de démarrage standard de la configuration du BIOS. Cette opération n'ouvre pas de menu, ni ne permet la gestion des périphériques réseau.