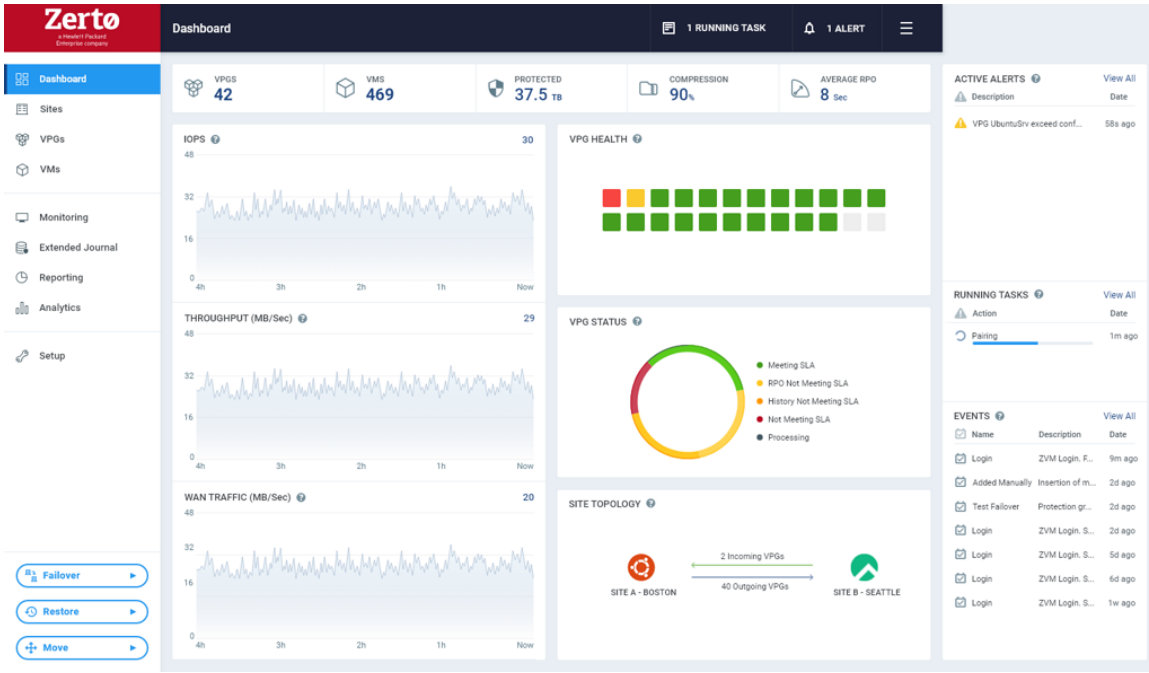
Fiche technique

HPE Zerto Software

HPE Zerto Software Enterprise Replication 1 VM Expansion 28-month Offline Subscription E-LTU (S7X04AAE)



Nouveautés

- Récupérez rapidement des sites entiers, sur site ou dans le cloud, en quelques minutes sans perturber l'activité. Les organisations font confiance à HPE Zerto pour une protection fiable contre les perturbations dans tous les secteurs.
- HPE Zerto Software for AWS et Azure simplifie désormais la gestion à l'échelle de l'entreprise, en prenant en charge des milliers de machines virtuelles pour la protection dans, vers ou depuis l'infrastructure de cloud public.
- HPE Zerto In-Cloud Software for AWS fournit désormais une reprise après

Vue d'ensemble

Souhaitez-vous réduire votre temps d'arrêt, améliorer la reprise après incident et attaque par ransomware, garantir la disponibilité de vos données ou migrer vos charges de travail facilement ? HPE Zerto Software fournit des logiciels de reprise après sinistre, de cyber-résilience et de mobilité de la charge de travail pour les environnements virtualisés et cloud. HPE Zerto Software est conçu pour offrir une protection et une réplication continues des données, garantissant ainsi une reprise rapide des activités avec des temps d'arrêt de quelques minutes et des pertes de données de quelques secondes.
HPE Zerto est conçu pour prendre en charge une large gamme d'environnements IT, notamment VMware®, Hyper-V® et les clouds publics tels qu'AWS® et Microsoft Azure®. La plateforme offre une solution unifiée et évolutive qui simplifie la complexité liée à la protection des données, permettant aux organisations de protéger et de récupérer les applications et les données sur différentes infrastructures de manière transparente.

sinistre pour AWS dans l'ensemble des régions et des zones de disponibilité. La protection et la reprise peuvent facilement s'adapter à plus d'un millier d'instances AWS EC2.

- HPE Zerto Software améliore la reprise après sinistre grâce à la détection du cryptage en temps réel, à l'identification en quelques secondes des attaques de ransomware. Il offre également des copies de journaux immuables stockées en toute sécurité, à l'abri des attaquants.

- HPE Zerto permet une migration transparente des charges de travail vers une nouvelle infrastructure, un cloud public ou des prestataires de services, simplifiant le regroupement des datacenters et facilitant les déplacements vers, depuis et entre les clouds.

Caractéristiques

Protection des données en continu

La réplication quasi synchrone assurée par HPE Zerto préserve la protection des données en temps réel, fournissant des points de reprise mesurés en secondes, éliminant ainsi presque toute perte de données. Le journal de reprise HPE Zerto conserve des milliers de points de reprise pendant 30 jours maximum, offrant une reprise granulaire et flexible.

HPE Zerto simplifie la reprise des applications et la reprise sur site à l'aide de groupes de protection virtuels qui synchronisent la réplication et la reprise sur plusieurs machines virtuelles, créant des points de contrôle de reprise cohérents sur des ensembles entiers de machines virtuelles comprenant des applications complexes ou des sites entiers.

HPE Zerto automatise et orchestre la reprise pour éliminer presque entièrement les temps d'arrêt et les pertes de données. Qu'il s'agisse de protéger des dizaines ou des milliers de machines virtuelles, HPE Zerto offre des temps de récupération mesurés en minutes et des points de récupération mesurés en secondes.

HPE Zerto est intégré aux principaux fournisseurs de cloud, ce qui permet aux entreprises d'exploiter les ressources cloud pour la reprise après sinistre, la sauvegarde et la migration, offrant des solutions rentables et évolutives.

HPE Zerto fournit des outils d'analyse et de génération de rapports complets : les organisations disposent ainsi d'un aperçu de leur état de protection des données, de leurs performances de reprise et de leur conformité aux exigences réglementaires.

Mobilité multicloud

Protégez et migrez les charges de travail sur plusieurs plateformes, à la fois sur site et dans le cloud, grâce à des conversions automatisées transparentes de machines virtuelles sur les hyperviseurs et les plateformes d'infrastructure-as-a-service (IaaS).

Faites disparaître les obstacles et les soucis dans les projets de migration avec des temps d'arrêt proches de zéro. Migrez les applications et les données en temps réel sans impact sur la production et déplacez les charges de travail au sein d'architectures cloud hybrides et multicloud en toute confiance grâce à des tests non perturbateurs.

Évitez l'enfermement propriétaire grâce à une mobilité complète de la charge de travail vers, depuis ou au sein des plateformes sur site ou dans le cloud pour simplifier les architectures informatiques complexes.

Les conversions de machines virtuelles entre les plateformes sont effectuées automatiquement entre toutes les plateformes prises en charge pour une migration et une protection transparentes. Protégez, récupérez et migrez de grands groupes de machines virtuelles de manière simple et rapide.

Résilience face aux ransomwares

Détectez les attaques par ransomware en quelques secondes grâce à la détection de chiffrement en temps réel HPE Zerto qui alerte en cas d'activité de chiffrement anormale et crée des balises des points de reprise pour faciliter la reprise jusqu'à un point situé quelques secondes avant le début du chiffrement.

Créez des copies immuables du journal qui ne peuvent pas être modifiées par les pirates à l'origine d'attaques par ransomware pour empêcher la reprise.

Utilisez l'isolation du réseau pour la reprise, qui vous permet de valider et de corriger les données récupérées après une attaque de ransomware avant le retour en production.

Les organisations peuvent effectuer des tests de reprise après sinistre sans impacter les environnements de production, garantissant ainsi que les plans de reprise sont efficaces et à jour.

Gestion d'entreprise

HPE Zerto fournit des workflows hautement automatisés pour protéger, récupérer et tester la protection de centaines ou de milliers de machines virtuelles. Les groupes de protection virtuels sont utilisés pour orchestrer un grand nombre de machines virtuelles afin que des processus tels que les tests et la reprise puissent être effectués rapidement et en toute confiance en quelques clics seulement.

Les fonctionnalités d'orchestration de HPE Zerto permettent le regroupement logique des machines virtuelles dans des groupes de protection à récupérer individuellement ou en tant que groupe entier. Cela permet d'accélérer le processus de reprise et de garantir l'intégrité des données sur toutes les machines virtuelles d'un groupe de protection pour chaque point de contrôle de reprise.

HPE Zerto Analytics fournit une analyse de données basée sur le cloud dans une vue globale sur tous les sites HPE Zerto. Les données et les analyses fournissent des informations sur l'état de la protection et l'état de reprise, le tout dans une vue unifiée.

HPE Zerto garantit que des applications entières, et pas uniquement des machines virtuelles individuelles, sont protégées de manière cohérente, permettant une reprise transparente des applications complexes multi-VM. Adaptez-vous aux besoins de l'entreprise, en prenant en charge les environnements de petite et grande taille sur site et dans le cloud.

HPE Zerto est conçu pour s'adapter aux besoins de l'entreprise, prenant en charge les environnements de petite à grande échelle. Sa flexibilité permet de protéger les charges de travail dans les environnements sur site, hybrides et multicloud.

Caractéristiques techniques	HPE Zerto Software Enterprise Replication 1 VM Expansion 28-month Offline Subscription E-LTU
Product Number	S7X04AAE
Automatisation	L'automatisation désigne la capacité d'un logiciel à gérer des tâches qui devraient autrement être effectuées manuellement par un utilisateur. La réalisation manuelle des tâches est généralement plus longue et présente un risque plus élevé d'erreur humaine provoquant des perturbations, qui prolongent la durée ou retardent le projet. L'automatisation, qu'elle soit intégrée à une solution logicielle ou ajoutée via des scripts ou des outils tiers, peut accélérer les processus, éliminer les points d'erreur humaine au cours du processus et simplifier la gestion des charges de travail. L'automatisation de processus tels que la reprise après sinistre, les migrations ou les mises à jour du système peut réduire considérablement les temps d'arrêt et permettre une plus grande productivité pendant les fenêtres de maintenance.
AWS	Amazon Web Services (AWS) est une plateforme de cloud computing complète proposée par Amazon. Elle offre une large gamme de services, notamment de la puissance de calcul, des options de stockage et des capacités de mise en réseau, permettant aux entreprises et aux particuliers d'évoluer et d'innover efficacement. La plateforme AWS offre une sécurité stable, une infrastructure mondiale et des modèles de tarification flexibles, ce qui en fait un choix privilégié pour les organisations à la recherche de solutions cloud fiables et évolutives.
Azure	Microsoft Azure est une plateforme et un service de cloud computing complets proposés par Microsoft. Elle fournit une large gamme de services cloud, notamment l'informatique, l'analyse, le stockage et la mise en réseau. Les utilisateurs peuvent choisir et configurer ces services pour répondre à leurs besoins spécifiques, permettant le développement, le déploiement et la gestion d'applications via des datacenters gérés par Microsoft. Azure prend en charge divers langages de programmation, outils et frameworks, ce qui en fait une solution polyvalente pour les entreprises cherchant à tirer parti de la technologie cloud pour l'évolutivité, la flexibilité et l'innovation.
Continuité de l'activité	Un plan de continuité de l'activité est un cadre détaillant tous les événements qui surviendront en cas de perturbation des opérations commerciales. Il fait partie d'une politique de gestion des urgences qui relie la phase d'intervention d'urgence à la phase de reprise. Fondamentalement, un plan efficace de continuité de l'activité aide une organisation à faire face à l'inattendu. Dans la plupart des scénarios, les solutions impliquent le maintien de la redondance du système, le basculement et la reprise du poste de travail, et l'infrastructure IT y joue un rôle central essentiel. De la sauvegarde hors site aux plateformes partenaires cloud en passant par l'accès à distance, chaque aspect doit être soigneusement évalué et renforcé.
Cloud	Le cloud computing est une approche permettant de disposer de services informatiques via un réseau. Ce modèle permet d'accéder à la demande à tous types de ressources : stockage, serveurs, bases de données, réseau, logiciels, outils analytiques, applications, etc. Ces ressources sont généralement payables à l'utilisation, ce qui permet aux organisations de mettre en œuvre des solutions informatiques flexibles et évolutives sans avoir à gérer directement l'infrastructure sous-jacente. Le cloud computing facilite une utilisation efficace des ressources, ce qui permet aux entreprises d'adapter dynamiquement leurs capacités informatiques à l'évolution de la demande tout en optimisant les coûts.

Caractéristiques techniques	HPE Zerto Software Enterprise Replication 1 VM Expansion 28-month Offline Subscription E-LTU
Protection des données en continu	La protection continue des données utilise une technologie basée sur un journal pour conserver un journal de toutes les modifications survenant dans un laps de temps spécifié, offrant une reprise à tout moment par incréments de secondes et conserve ces données pendant une période spécifiée allant de quelques jours à plusieurs semaines. Contrairement aux systèmes hérités, qui accumulent des données périodiquement tout au long de la journée, puis tentent d'effectuer une sauvegarde pendant une fenêtre de temps, le système CDP sauvegarde constamment vos données. Par exemple, la reprise basée sur des snapshots expose votre entreprise à un risque de perte de données plus élevé en raison de points de restauration peu fréquents capturés, tandis que le système CDP minimise ce risque avec des milliers de points de restauration tout au long de l'historique du journal.
Cyberrésilience	La cyber-résilience est la capacité d'une entreprise à s'adapter aux cybermenaces, sans compromettre l'intégrité, la finalité et la continuité de l'activité. Elle représente le niveau de préparation d'une entreprise à l'anticipation et à la détection des cyber-attaques, ainsi qu'à la reprise qui s'ensuit. La cyber-résilience est essentielle à la protection des systèmes informatiques, des infrastructures critiques, des données et des applications des entreprises. Elle est importante parce qu'elle aide les entreprises à admettre que les pirates ont le dessus. Cette approche les oblige à se réconcilier avec les « inconnus inconnus » et à avoir une stratégie encore plus innovante, exhaustive et immédiate. Avec une cyber-résilience appropriée, les entreprises sont capables de fournir systématiquement les résultats escomptés malgré les cyber-événements indésirables.
Mobilité des données	La mobilité des charges de travail peut se référer à la fois aux projets de protection des données et de migration qui déplacent des charges de travail telles que des machines virtuelles sur différents sites, différents hyperviseurs et différents clouds. Les organisations, que ce soit par conception ou par le biais de fusions et acquisitions, peuvent s'appuyer des architectures informatiques complexes couvrant plusieurs plateformes. La mobilité de la charge de travail signifie une transition transparente d'une charge de travail d'une plateforme à une autre en quelques minutes pour éviter toute interruption prolongée. Un plan de protection des données peut récupérer les charges de travail d'un hyperviseur local vers une infrastructure de cloud public en tant que plateforme de service, ou un plan de migration peut déplacer les charges de travail d'une plateforme cloud vers un cloud différent. Les cas d'utilisation impliquent le déplacement de charges de travail vers, depuis ou même au sein de différentes plateformes sur site ou cloud de la manière la plus simple possible et avec un minimum de temps d'arrêt.
Protection des données	La protection des données est une combinaison de technologies telles que le clustering haute disponibilité, la reprise après sinistre et les technologies de sauvegarde qui protègent contre la perte et les perturbations des données. Les catastrophes naturelles, les erreurs humaines et les acteurs malveillants constituent tous une menace pour les données et la disponibilité des services informatiques. Un plan de protection des données pour une organisation vise à limiter les temps d'arrêt et les pertes de données et à se conformer à la réglementation gouvernementale en matière de protection des données. Les solutions de haute disponibilité protègent souvent contre les pannes matérielles, les solutions de reprise après sinistre protègent contre toute interruption, même au niveau multisite, et les solutions de sauvegarde assurent la récupération de données pour se conformer aux réglementations pour une conservation des données à long terme pouvant durer des années.

Caractéristiques techniques	HPE Zerto Software Enterprise Replication 1 VM Expansion 28-month Offline Subscription E-LTU
Reprise après sinistre	En informatique, la reprise après sinistre (DR) fait référence aux stratégies, processus, produits et solutions que vous mettez en place pour récupérer et protéger l'infrastructure IT d'une entreprise en cas de sinistre. Cela comprend les catastrophes naturelles, les cyberattaques, les pannes matérielles et autres événements catastrophiques. La reprise après sinistre est essentielle car elle minimise les temps d'arrêt en cas de sinistre et protège l'intégrité des données. Il aide les entreprises à reprendre rapidement leurs opérations et à réduire l'impact des interruptions. Toutes les entreprises devraient disposer d'un plan de reprise après sinistre pour garantir la continuité de l'activité.
Restauration	La restauration automatique fait référence au processus de retour de votre système de son emplacement secondaire à son emplacement principal. Bien que la restauration automatique fasse parfois partie de la maintenance planifiée, elle constitue un élément crucial de la reprise après sinistre. Après une catastrophe, le retour arrière se produit souvent après le basculement.
Basculement	Le basculement consiste à récupérer les opérations informatiques sur un système secondaire lorsque votre système principal tombe en panne. La panne peut être due à de nombreuses raisons, mais les principales sont les pannes de courant et de réseau, les catastrophes naturelles et les ransomwares. Le basculement des systèmes informatiques, également appelé basculement de reprise après sinistre, est un élément essentiel de la continuité de l'activité.
Hyperviseur	Un hyperviseur, également connu sous le nom de gestionnaire de machines virtuelles (VMM), est un logiciel qui permet à plusieurs machines virtuelles (VM) de partager les ressources d'un seul serveur. Cette couche logicielle permet à plusieurs machines virtuelles (VM) de s'exécuter sur le même matériel hôte, optimisant ainsi l'exploitation des ressources de calcul. Les ressources de l'hôte, telles que l'unité centrale, le processeur graphique, la mémoire, l'espace de stockage et la bande passante réseau, sont allouées de manière dynamique aux différentes machines virtuelles exécutées sur celle-ci. Sans hyperviseurs, la virtualisation ne serait tout simplement pas possible.
Orchestration	L'orchestration désigne la capacité à gérer plusieurs charges de travail ensemble en tant que groupe. Il s'agit par exemple de la récupération ou de la migration d'un grand nombre de charges de travail ou de plusieurs sites informatiques de manière unifiée. L'orchestration est souvent associée à l'automatisation sur de grands groupes de charges de travail où les règles et les politiques peuvent être définies ou modifiées pour le groupe plutôt que de manière individuelle. Une application complexe de grande taille, par exemple, peut s'étendre sur de nombreuses charges de travail qui doivent toutes être protégées ou migrées comme un groupe complet pour garantir l'intégrité des données et maintenir les dépendances entre les charges de travail.
Résilience face aux ransomwares	La résilience face aux ransomwares désigne la capacité d'une organisation à réagir rapidement à une attaque de ransomware et à récupérer les données en toute confiance pour limiter les interruptions et éviter le versement d'une rançon. Les attaques par ransomware s'appuient sur des temps de reprise lents ou empêchent complètement la reprise pour exiger d'énormes rançons pour la récupération de données. La résilience face aux ransomwares est essentielle pour éviter les interruptions qui ont des répercussions financières et sur la fidélité à la marque d'une organisation. Un plan de résilience face aux ransomwares doit inclure une détection précoce dès le début d'une attaque, la création de copies de données immuables pour la reprise et la possibilité de récupérer les données dans un environnement réseau isolé auquel les attaquants n'ont aucun accès.

Caractéristiques techniques	HPE Zerto Software Enterprise Replication 1 VM Expansion 28-month Offline Subscription E-LTU
Objectif de point de récupération (RPO)	Le RPO mesure la perte de données dans un scénario de reprise après sinistre. Il se réfère au point le plus récent dans le temps auquel une bonne copie connue des données est disponible pour récupérer un système. Plus un point de reprise remonte loin dans le temps, plus le volume de données perdues est important. Le RPO qui peut être atteint est souvent déterminé par la solution de protection des données utilisée, comme : les sauvegardes, la réplication du stockage ou la réplication de données en continu.
Objectif de délai de reprise (RTO)	Le RTO représente la durée d'indisponibilité attendue avant que les opérations, y compris les services de données et d'application, soient de nouveau en ligne après une interruption. Le RTO peut être influencé par de nombreux facteurs, notamment le niveau des processus de reprise manuels et automatisés tels que l'ordre de démarrage des machines virtuelles, la redirection du trafic réseau, la récupération cohérente des piles d'applications et autres.
Support de réplication	La réplication est un processus de copie de données d'un emplacement de données à un autre, souvent utilisé pour faciliter la protection des données ou les projets de migration. La réplication peut détecter et dupliquer des données de manière périodique ou en continu afin de créer une copie des données dans un autre emplacement. A la différence d'une copie de fichier typique qu'un utilisateur peut effectuer, la réplication couvre généralement de grands ensembles de données ou englobe des charges de travail entières comme des machines virtuelles et inclut des métadonnées sur la charge de travail. La réplication est généralement effectuée à grande échelle en déplaçant de grands volumes de données, soit pour un déplacement ponctuel spécifique des données, soit de manière continue pour maintenir une copie à jour d'un ensemble de données dans un emplacement secondaire pour la reprise ou la distribution des données.
VMware	VMware, Inc. est un prestataire de premier plan de solutions de virtualisation et de cloud computing. Fondée en 1998, la société VMware a joué un rôle essentiel dans la transformation du paysage informatique en permettant aux organisations d'exécuter plusieurs machines virtuelles sur un seul serveur physique, optimisant ainsi l'utilisation des ressources et réduisant les coûts.
Mobilité multicloud	La mobilité multicloud fait référence à la capacité de gestion, de migration et d'intégration transparentes des applications, des données et des services dans plusieurs environnements cloud. Il s'agit de tirer parti des atouts de différents prestataires cloud pour optimiser les performances, les coûts et la résilience. Grâce aux caractéristiques d'interopérabilité et de flexibilité, la mobilité multicloud permet aux organisations d'éviter l'enfermement propriétaire, d'améliorer les fonctionnalités de reprise après sinistre et d'adapter les solutions cloud aux besoins spécifiques de l'entreprise.
Migration cloud	La migration cloud fait référence au processus de déplacement des données, des applications et des ressources informatiques d'une organisation depuis une infrastructure sur site ou des systèmes hérités vers des environnements basés sur le cloud. Cette transition permet aux entreprises de tirer parti de l'évolutivité, de la flexibilité et de la rentabilité offertes par le cloud computing, tout en facilitant une meilleure collaboration, une sécurité renforcée et l'accès à des technologies avancées. La migration cloud peut impliquer diverses stratégies, telles que le réhébergement, la refactorisation ou la réarchitecture, en fonction des besoins et des objectifs spécifiques de l'organisation.

Caractéristiques techniques	HPE Zerto Software Enterprise Replication 1 VM Expansion 28-month Offline Subscription E-LTU
Plates-formes prises en charge	HPE Zerto Software prend en charge les plateformes de virtualisation VMware vSphere, Microsoft Hyper-V, Amazon Web Services (AWS) et Microsoft Azure pour la protection et la migration des données. Pour consulter la liste complète des versions de plateformes de virtualisation, des systèmes d'exploitation pris en charge et des fonctionnalités compatibles avec les différentes versions de HPE Zerto, veuillez vous référer à la matrice d'interopérabilité HPE Zerto Software. Les fonctionnalités ci-dessous font toutes partie des solutions fournies par HPE Zerto Software dans le cadre de la gamme des produits de protection des données de HPE.

Pour plus d'informations techniques, les modèles disponibles et les options, veuillez vous référer aux QuickSpecs

Visiter HPE.com

Dialoguer en ligne

© Copyright 2026 Hewlett Packard Enterprise Development LP. Les informations contenues dans ce document sont sujettes à modification sans préavis. Les seules garanties relatives aux produits et services Hewlett Packard Enterprise sont stipulées dans les déclarations de garantie expresses accompagnant ces produits et services. Aucune déclaration contenue dans ce document ne peut être interprétée comme constituant une garantie supplémentaire. Hewlett Packard Enterprise décline toute responsabilité en cas d'erreurs ou d'omissions de nature technique ou rédactionnelle dans le présent document.

Pièces et équipements : HPE fournira les pièces de rechange et le matériel nécessaires à l'entretien des équipements couverts.

Les pièces et les composants dont la durée de vie prise en charge maximale et/ou les limites d'utilisation maximale sont atteintes, conformément à ce qui est indiqué dans le manuel d'utilisation du fabricant, dans la fiche de présentation des caractéristiques techniques ou dans la fiche de description technique, ne seront pas fournis, réparés ou remplacés.

Microsoft, Azure et Hyper-V sont des marques commerciales du groupe Microsoft.; Amazon Web Services, AWS et le logo Powered by AWS sont des marques commerciales d'Amazon.com, Inc. ou de sa filiale.; VMware est une marque déposée ou une marque commerciale de VMware, Inc. aux États-Unis et/ou dans d'autres pays.; SAP S/4HANA est la marque commerciale ou déposée de SAP SE ou de ses filiales en Allemagne et dans d'autres pays.

L'image peut être différente du produit réel.

PSN1014953011FRFR, octobre, 2026.

HEWLETT PACKARD ENTERPRISE

hpe.com