Power Systems

Amorçage sécurisé dans PowerVM

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 11.

Cette édition s'applique à IBM® AIX version 7.2, IBM AIX version 7.1, IBM AIX version 6.1, IBM i 7.4 (numéro de produit 5770-SS1), IBM Virtual I/O Server version 3.1.1, ainsi qu'à toutes les versions et modifications ultérieures, sauf mention contraire dans les nouvelles éditions. Cette version ne s'exécute pas sur tous les modèles d'ordinateur à jeu d'instructions réduit (RISC) ni sur les modèles CISC.

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Les informations qui y sont fournies sont susceptibles d'être modifiées avant que les produits décrits ne deviennent eux-mêmes disponibles. En outre, il peut contenir des informations ou des références concernant certains produits, logiciels ou services non annoncés dans ce pays. Cela ne signifie cependant pas qu'ils y seront annoncés.

Pour plus de détails, pour toute demande d'ordre technique, ou pour obtenir des exemplaires de documents IBM, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial.

Vous pouvez également consulter les serveurs Internet suivants :

- http://www.fr.ibm.com (serveur IBM en France)
- http://www.ibm.com/ca/fr (serveur IBM au Canada)
- http://www.ibm.com (serveur IBM aux Etats-Unis)

Compagnie IBM France
Direction Qualité
17, avenue de l'Europe
92275 Bois-Colombes Cedex

Table des matières

Avis aux lecteurs canadiens

Le présent document a été traduit en France. Voici les principales différences et particularités dont vous devez tenir compte.

Illustrations

Les illustrations sont fournies à titre d'exemple. Certaines peuvent contenir des données propres à la France.

Terminologie

La terminologie des titres IBM peut différer d'un pays à l'autre. Reportez-vous au tableau ci-dessous, au besoin.

IBM France	IBM Canada
ingénieur commercial	représentant
agence commerciale	succursale
ingénieur technico-commercial	informaticien
inspecteur	technicien du matériel

Claviers

Les lettres sont disposées différemment : le clavier français est de type AZERTY, et le clavier français-canadien de type QWERTY.

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

- les pages de codes 850 (multilingue) et 863 (français-canadien),
- le code pays 002,
- le code clavier CF.

Nomenclature

Les touches présentées dans le tableau d'équivalence suivant sont libellées différemment selon qu'il s'agit du clavier de la France, du clavier du Canada ou du clavier des États-Unis. Reportez-vous à ce tableau pour faire correspondre les touches françaises figurant dans le présent document aux touches de votre clavier.

France	Canada	Etats-Unis
↖ (Pos1)	↖	Home
Fin	Fin	End
⇞ (PgAr)	⇞	PgUp
⇟ (PgAv)	⇟	PgDn
Inser	Inser	Ins
Suppr	Suppr	Del
Echap	Echap	Esc
Attn	Intrp	Break
Impr écran	ImpEc	PrtSc
Verr num	Num	Num Lock
Arrêt défil	Défil	Scroll Lock
(Verr maj)	FixMaj	Caps Lock
AltGr	AltCar	Alt (à droite)

Brevets

Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, vos demandes de renseignements relatives aux permis d'utilisation au directeur général des relations commerciales d'IBM, 3600 Steeles Avenue East, Markham, Ontario, L3R 9Z7.

Assistance téléphonique

Si vous avez besoin d'assistance ou si vous voulez commander du matériel, des logiciels et des publications IBM, contactez IBM direct au 1 800 465-1234.

Amorçage sécurisé dans PowerVM

Les serveurs IBM Power Systems fournissent une plateforme de serveur hautement sécurisé. Le matériel et le microprogramme à processeur IBM POWER9 incluent de nouvelles fonctions PowerVM afin de fournir une plateforme plus sécurisée pour le déploiement en cloud.

Les fonctions PowerVM clé disponibles sur les serveurs à processeur POWER9 incluent :

- Un processus d'IPL sécurisé ou la fonction d'amorçage sécurisé qui autorise uniquement l'exécution sur les processeurs système des composants de microprogramme appropriés. Chaque composant de la pile de microprogramme, notamment l'amorçage hôte (hostboot), l'hyperviseur POWER (PHYP) et le microprogramme de partition (PFW), est signé par le fabricant de la plateforme et vérifié dans le cadre du processus d'IPL.
- Une infrastructure destinée à prendre en charge l'attestation à distance de la pile du microprogramme du système via un module TPM matériel.

Amorçage sécurisé et amorçage digne de confiance

Pour cette documentation, les termes *amorçage sécurisé (Secure Boot)* et *amorçage digne de confiance (Trusted Boot)* possèdent des connotations spécifiques. Ils sont utilisés comme des concepts distincts mais complémentaires.

Amorçage sécurisé
: La fonction Amorçage sécurisé protège l'intégrité du système en utilisant des signatures numériques pour effectuer une vérification protégée par le matériel de tous les composants de microprogramme. Cette fonction fait également la distinction entre le domaine de confiance du système et le domaine de confiance du processeur de service flexible (FSP) en contrôlant l'accès du processeur de service et de l'interface de service aux régions de mémoire système sensibles.

Amorçage digne de confiance
: La fonction d'amorçage sécurisé crée des mesures de plateforme protégées et fortes d'un point de vue cryptographique, qui prouvent que des composants de microprogramme spécifiques ont été exécutés sur le système. Vous pouvez évaluer les mesures en utilisant des protocoles sécurisés pour déterminer l'état du système et utiliser ces informations pour prendre des décisions en matière de sécurité.

Amorçage sécurisé dans PowerVM - Nouveautés

Prenez connaissance des informations nouvelles ou modifiées de l'ensemble de rubriques Amorçage sécurisé dans PowerVM depuis la mise à jour précédente.

Août 2018

- Diverses mises à jour ont été apportées à cet ensemble de rubriques.

Termes

Présentation des termes utilisés dans cette documentation.

Auxiliaire
: Partition enfant qui utilise l'UC allouée à une autre partition. Un adjoint est immédiatement disponible pour l'administrateur système et peut être utilisé pour servir la partition principale.

Alter/Display Unit (ADU)
: Ressource matérielle utilisée pour accéder au stockage principal. Une unité ADU est utilisée par les éléments matériels et logiciels.

Conteneur de code
Image de code vérifiable qui possède un en-tête de préfixe d'amorçage sécurisé. Le conteneur est une structure composée d'un en-tête de préfixe 4K (en-tête matériel, en-tête de clé de préfixe, ou en-tête de microprogramme), suivi d'un contenu protégé (une image de code qui comporte un hachage dans l'en-tête de préfixe), ainsi que toute donnée utile unique au serveur.

Autorité de signature de code
Niveau d'autorisation accordé aux individus connaissant le code objet pour activer la distribution d'un rôle en tant que signataire autorisé pour les fonctions serveur de signature.

Core Root of Trust for Measurement (CRTM)
Code (non modifiable) sécurisé par priorité, qui fait partie des donnée d'identification de la plateforme. Dans le modèle RTM statique, le code CRTM doit être exécuté en premier quand le serveur ou l'environnement matériel physique est mis sous tension, ou quand le serveur ou l'environnement matériel physique est réinitialisé. Pour la fonction d'amorçage sécurisé, le code CRTM est basé sur le moteur d'amorçage auto/hostboot (SBE/HB). Le code CRTM inclut le moteur d'amorçage auto et suffisamment de code hostboot pour autoriser un pilote d'unité TPM à s'initialiser.

Console de gestion
Interface permettant aux administrateurs système et représentants de service d'afficher et d'exécuter des tâches sur le matériel, le partitionnement, ainsi que des aspects liés à la maintenance d'un système.

Processeur maître
Processeur du noeud qui est physiquement connecté à la mémoire flash not-OR (NOR).

Extension PCR
Opération effectuée sur les registres de configuration de plateforme (PCR) TPM afin de mettre à jour la valeur de registre pour enregistrer l'historique des messages étendus au registre. Plutôt que d'effectuer l'opération d'écriture directement sur un registre PCR, l'opération d'extension PCR prend la valeur d'origine dans le PCR, concatène le nouveau message avec, puis prend une valeur de hachage pour produire une valeur de registre mise à jour. L'historique des messages étendu et l'ordre des extensions peut être comparé ultérieurement avec les journaux d'événements correspondants.

Certificat de plateforme
Certificat qui existe dans le module TPM et qui certifie que la plateforme associée au TPM est une plateforme IBM avec un code CRTM. Le certificat ne dépend pas du modèle de plateforme.

PNOR
Processor not-OR (PNOR), également appelé flash.

En-tête de préfixe
Structure de 4 Ko qui est préfixée sur les images de code signé des conteneurs de code d'amorçage sécurisé.

Clé privée pour la signature du code
Portion privée ou secrète d'une paire de clés publique/privée utilisée pour le chiffrement à clé publique, via des algorithmes de clé asymétrique.

Registres protégés
Registres en lecture seule via la communication d'analyse (SCOM) par le processeur de service flexible (FSP) mais sont lus/écrits à l'aide de code sécurisé. Dans la plupart des cas, ces registres sont indépendants de la valeur analysée lors de l'initialisation et ont par défaut une valeur connue.

Clé publique de signature du code
Portion publique/privée d'une paire de clés publique/privée utilisée pour le chiffrement à clé publique, via des algorithmes de clé asymétrique.

Attestation à distance
Vérifie quels logiciels sont en cours d'exécution sur un ordinateur distant. L'attestation est le processus de validation de l'exactitude des informations. L'attestation à distance permet aux parties prenantes autorisées de déterminer les modifications apportées à l'ordinateur de l'utilisateur, en vérifiant le statut du module TPM et de la plateforme sur lesquels elle réside.

Self Boot Engine (SBE)
Moteur de réinitialisation à la mise sous tension utilisé pour l'initialisation de la puce processeur pour exécuter des procédures hostboot.

Signature
Démontre l'authenticité d'un message. La signature se compose du hachage du message objet chiffré avec une moitié d'une paire de clés publique/privée.

Static Root of Trust for Measurement (SRTM)
Un système s'amorce depuis une portion non modifiable du code du microprogramme qui est considéré comme digne de confiance à tout moment. L'action d'amorçage initie le processus de mesure dans lequel chaque composant mesure le prochain composant d'une chaîne.

Blocs de construction sécurisés (TBB)
Inclut les portions des racines de mesure de confiance (RTM) qui ne disposent pas d'emplacements protégés ou de fonctionnalités protégées. TBB inclut la mesure CRTM, la connexion du stockage CRTM à une carte système, la connexion du module TPM à une carte système, ainsi que des mécanismes destinés à déterminer la présence physique de l'utilisateur.

Code sécurisé
Microprogramme autorisé par du matériel IBM prédésigné et des droits d'accès au microprogramme. La source du code est authentifiée et l'intégrité de l'image est vérifiée.

Trusted Computing Group (TCG)
Trusted Computing Group est une organisation à but non lucratif formée pour développer, définir et promouvoir des normes de l'industrie mondiale ouvertes et non liées à des fournisseurs, qui soutient une mesure RTM (Root of Trust Measurement) basée sur le matériel pour des plateformes de calcul fiables et interopérables.

Mémoire sécurisée
Région de mémoire accessible (en lecture et en écriture) uniquement à dus code sécurisé. L'accès à la mémoire sécurisée est bloqué par des mécanismes d'isolement du matériel quand lors d'amorçage système en mode sécurisé. Une petite section de la mémoire qui se trouve hors de la région de mémoire sécurisée est appelée *mémoire non sécurisée* et peut être accessible facilement aux interfaces de service pour effectuer des opérations de lecture et d'écriture.

Module TPM (Trusted Platform Module)
Coprocesseur cryptographique à faible performance, de type carte à puce. Un module TPM peut stocker des hachages de la séquence d'amorçage dans un ensemble de registres PCR (Platform Configuration Register).

Mémoire non sécurisée
Région de mémoire avec un accès ouvert en lecture et en écriture qui inclut le processeur FSP et des interfaces de service qui existent hors du domaine de sécurité des processeurs hôte.

Validation
Pour vérifier l'identité du signataire, par exemple, la validation d'un conteneur de code signifie vérifie que le code de l'image contenue est numériquement signé par IBM et que l'image n'a pas été modifiée.

Code de vérification
Du code protégé existe dans la mémoire morte SEEPROM (mémoire morte reprogrammable série) et fournit la prise en charge de la vérification de signature pour les conteneurs de code d'amorçage sécurisé. Le code de vérification est l'élément clé utilisé pour établir la racine principal de confiance pour la mesure durant l'amorçage sécurisé.

Processus d'IPL (procédure de chargement initial)

La fonction d'amorçage sécurisé (Secure Boot) empêche l'accès non autorisé aux données client, que ce soit via un microprogramme non autorisé s'exécutant sur un processeur système ou d'un accès via des vulnérabilités en matière de sécurité au niveau du microprogramme autorisé du processeur de service, ou encore via des interfaces de maintenance du matériel à l'aide du processeur FSP (processeur de service flexible).

Si l'amorçage sécurisé empêche l'accès non autorisé aux données clients, ses mécanismes n'offrent pas de protection contre les menaces suivantes :

- Les attaques basées sur le logiciel du système d'exploitation visant à obtenir un accès non autorisé aux données client.
- Les administrateurs système sans scrupules.
- Les attaques physiques du matériel (par exemple, les substitutions de puce ou l'enregistrement du trafic des bus).

La fonction Amorçage sécurisé implémente une chaîne de confiance basée processeur dans le matériel processeur POWER9 qui est activée par la pile de microprogramme POWER9. La fonction Amorçage sécurisé fournit une base de microprogramme sécurisée afin d'améliorer la confidentialité et l'intégrité des données client dans un environnement virtualisé.

La fonction d'amorçage digne de confiance des serveurs à processeur POWER9 permet de mesurer la le code de chemin de la configuration du système et de l'IPL, et ces mesures peuvent ultérieurement servir de preuve via l'attestation de la configuration d'IPL initial du système. Pour créer des mesures Core Root of Trust for these Measurements (CRTM), un flux Amorçage sécurisé est utilisé pour ajouter des vérifications cryptographique à chaque phase du processus d'IPL jusqu'à ce que la communication avec le module TPM (Trusted Platform Module) soit établie. Le flux Amorçage sécurisé garantit l'intégrité de tout le microprogramme qui doit être utilisé sur des processeurs coeur et, de ce fait, empêche l'exécution de tout microprogramme non autorisé modifié de manière malveillante. Un échec d'authentification du code à un point quelconque empêche le processus d'IPL d'aboutir.

La fonction Amorçage sécurisé des systèmes POWER9 établit la confiance via le processus d'amorçage de la plateforme. Ici, *digne de confiance* signifie que le code exécuté durant le processus d'IPL provient du fabricant de la plateforme, est signé par ce fabricant et n'a pas été modifié.

La protection du mode sécurisé disponible sur des serveurs à processeur POWER9 conserve la fiabilité en empêchant l'accès en lecture/écriture aux données client par le processeur FSP et les interfaces de service, en empêchant l'exécution de code non fiable sur le processeur hôte, et en conservant la confiance sur tous les points clé du processus d'amorçage sécurisé.

La fonction POWER9 Amorçage sécurisé implémente une chaîne de confiance basée processeur. Cette chaîne débute par un composant implicitement digne de confiance, tandis que d'autres composants sont authentifiés et leur intégrité est vérifiée avant qu'ils ne soient exécutés sur les coeurs du processeur hôte. Le code de vérification qui se trouve dans le processeur verrouillé de la mémoire moire Serial Electrically Erasable Programmable ROM (SEEPROM) valide la charge initiale du microprogramme. Le microprogramme vérifie les signatures cryptographiques de tout microprogramme ultérieur qui doit être sécurisé et qui est chargé pour exécution sur les coeurs processeur POWER9. Sur un système POWER9, les options de sécurité SEEPROM sont définies dans le code SBE (Self-Boot Engine) et fixées sur la ligne d'assemblage (fabricant) du système afin de fournir la base à la mise en application matérielle de flux d'IPL sécurisés. Des cavaliers de mode de sécurité physique sont disponibles sur le *circuit électronique arrière* d'un système. Ces cavaliers peuvent être utilisés pour remplacer les commutateur de mode sécurisé du processeur si une personne accède physiquement au système. Le processus d'IPL sécurisé améliore encore davantage le calcul sécurisé sur la plateforme Power.

Le diagramme suivant illustre les opérations d'un processus d'IPL STB.

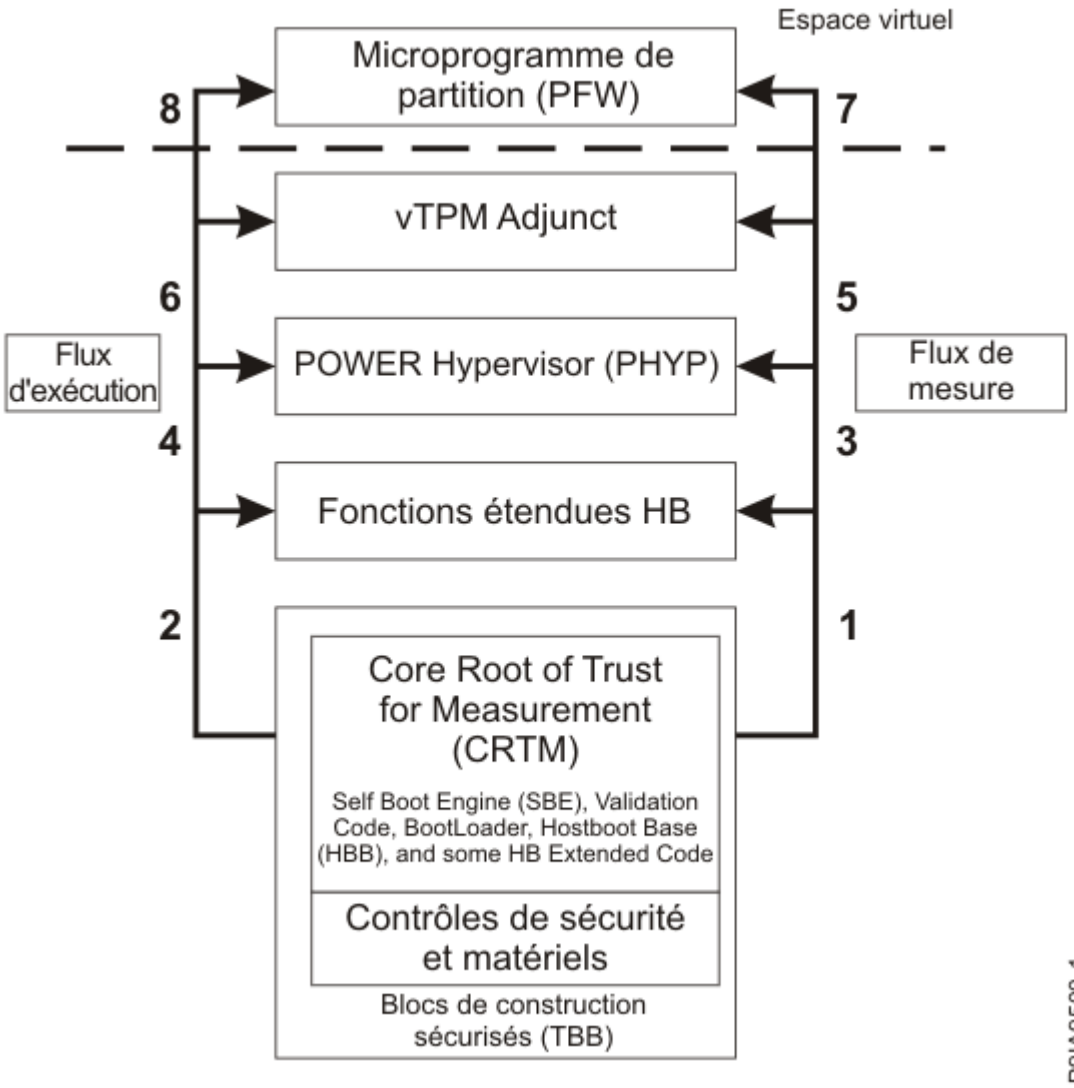

Figure 1. Flux Secure and Trusted Boot

La fonction Amorçage sécurisé établit le code de base SEEPROM, SBE et hostboot verrouillé (incluant une petite partie du code étendu d'amorçage hôte) comme racine Core Root of Trust for Measurement (CRTM), avec la chaîne de confiance étendue pour inclure POWER Hypervisor (PHYP), le microprogramme de partition (PFW), une sélection de partitions adjointes (module TPM physique (pTPM), module TPM virtuel (vTPM), exécution d'amorçage hôte et adjoints de chiffrement), et un contrôleur OCC (On Chip Controller - gestion thermique). Ce domaine de confiance et la prise en charge de la sécurité matérielle des processeurs garantissent que les données client ne sont pas affichées ou modifiées via des mécanismes matériels ou de microprogramme.

La pile de microprogramme sécurisé complète est authentifiée via des images signées et est exécutée à des emplacements de mémoire sécurisés. Le processeur FSP est gardé hors du domaine de confiance du serveur hôte et il ne peut pas accéder aux registres ADU (Alter/Display Unit), d'autres registres protégés ou aux régions de mémoire sécurisées. Le moteur Self Boot Engine (SBE) applique le blocage du processeur FSP en filtrant la liste noire des fonctions SCOM de lecture/écriture dans les registres. Les fonctions SCOM sont activées par le commutateur d'accès sécurisé de la zone SEEPROM de la puce du processeur.

La figure suivante représente un environnement à amorçage sécurisé.

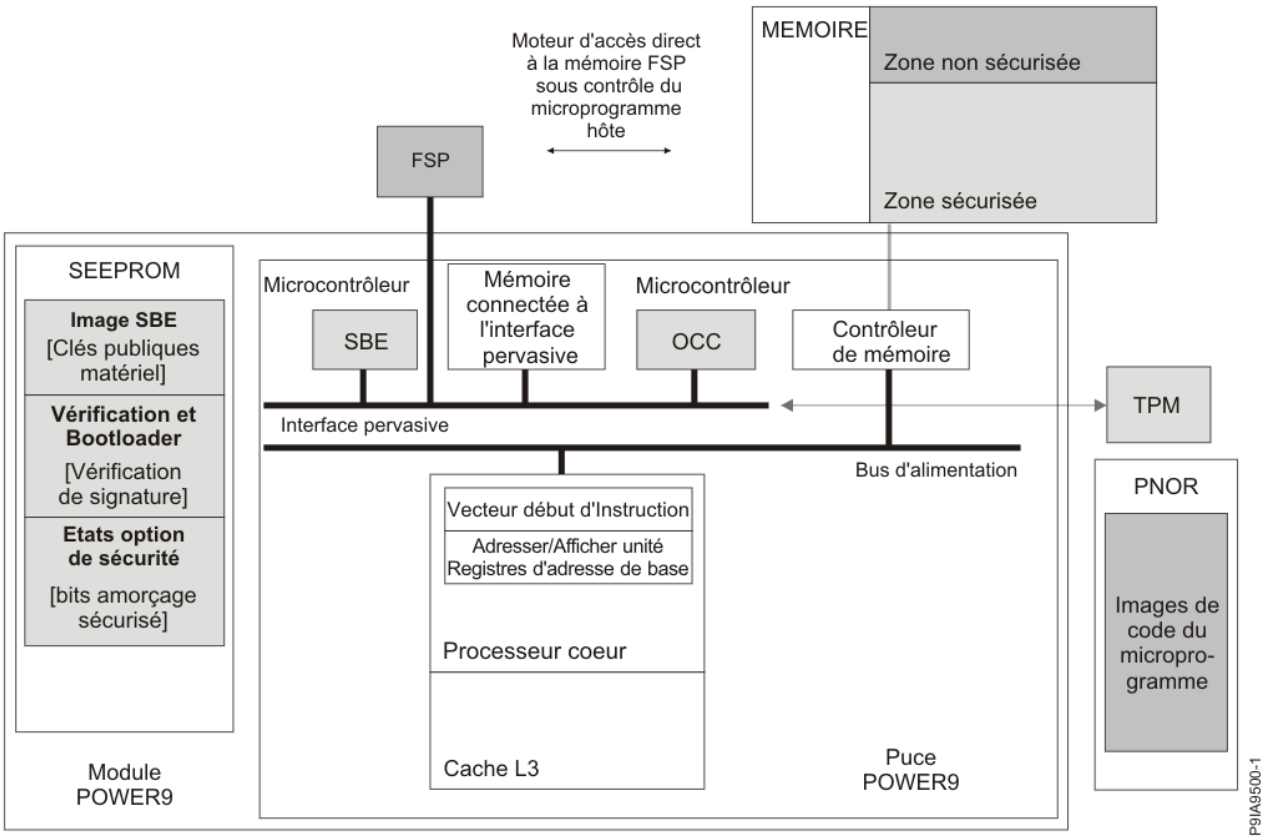

Figure 2. Environnement d'amorçage sécurisé

Quand le processus d'amorçage sécurisé débute, l'élément FSP envoie une demande d'amorçage et des détails sur le type d'amorçage aux puces processeur du système. En interne, les valeurs précédemment définies de l'état de la logique Amorçage sécurisé sont effacées pour partir d'un état connu approprié. Toute demande tempérée exécutée précédemment est également effacée de l'état. Des mécanismes de protection du matériel sont implémentées afin d'empêcher un agresseur informatique malveillant d'ignorer cette étape initiale. L'accès depuis le processeur FSP aux ressources de puce internes est verrouillé et le moteur d'amorçage sécurisé commence l'extraction du code d'initialisation depuis la mémoire qui est sur module, sécurisée, rémanent et verrouillée. Ce code effectue l'initialisation de base des puces et réinitialise le module TPM.

Une fois l'étape initiale du processus d'amorçage terminée, le moteur SBE (Self Boot Engine) charge le programme de chargement hostboot et le code de validation depuis la mémoire SEEPROM dans le cache de niveau 3 interne de la puce processeur. Un coeur de processeur est ensuite démarré et le programme de chargement d'amorçage extrait le code HBB (Host Boot Base) initial de la puce flash PNOR (Processor NOR) et le charge dans le cache L3. En mode sécurisé, le code de validation provenant du cache L3 est utilisé pour vérifier l'image HBB qui est à présent disponible dan le cache sécurisé. Une fois le code flash initial vérifié, le coeur de processeur continue d'exécuter le code validé depuis l'espace mémoire sécurisé et charge et valide les fonctions étendues HB (HBI). Une fois le HBI mesuré et la signature vérifiée et copiée, sa mesure (hachage d'image), indiquant l'authentification valide, est enregistrée dans le module TPM, comme indiqué par l'**Etape 1** de la Figure Flux Secure and Trusted Boot. A ce stade, tout le code exécuté est entièrement contenu dans la puce flash PNOR et aucun autre mécanisme n'a accédé au système. Il s'agit de la frontière de l'amorçage sécurisé. En cas d'échec de la vérification, le système est immédiatement arrêté et est protégé par des mécanismes de protection du matériel afin d'empêcher l'exécution de code non fiable ou indésirable.

Le code HB gère ensuite les mises à jour en attente pour la mémoire rémanente sécurisée en utilisant une nouvelle image sécurisée. Pour protéger la mesure CRIM, le code HB verrouille la mémoire sécurisée, empêchant ainsi tout nouvel accès en écriture à cette mémoire (cette action signifie que, si le système est réamorcé, il revient à cet état de confiance). Le code HB initialise ensuite le contrôleur de mémoire sur puce et les barrettes DIMM. Le code HB initialise également d'autres puces directement connectées au

processeur sur lequel il s'exécute, avant d'établir l'interface cohérente de mémoire avec les autres puces du système. Ces autres puces sont également vérifiées afin de s'assurer qu'elles sont dans un état sécurisé et digne de confiance.

Les composants supérieurs de la pile de microprogramme sont ensuite chargés, vérifiés, exécutés, et leurs mesures sont enregistrées dans le module TPM. Cette action termine l'**Etape 2**, indiquée à la Figure Flux Secure and Trusted Boot. A l'**Etape 3** de la figure Flux Secure and Trusted Boot, le contenu de POWER Hypervisor (PHYP) est chargé dans la mémoire principale. Le code est ensuite authentifié de manière cryptographique et après que l'authentification a abouti, l'hyperviseur PHYP débute son exécution. La mesure d'authentification du code PHYP est enregistrée dans le module TPM. De la même façon, les **étapes 4 à 8** de la Figure Flux Secure and Trusted Boot sont effectuées pour charger le code depuis la mémoire flash déverrouillée vers la mémoire sécurisée, le code est authentifié de manière cryptographique, puis différents adjoints et microprogramme de partition sont exécutés.

Prise en charge du module TPM en mode sécurisé

Le module TPM (Trusted Platform Module) active l'attestation à distance de la pile de code sur un système en cours d'exécution. Le microprogramme de la chaîne de confiance enregistre le hachage du microprogramme chargé et stocke les enregistrements sur le réseau des modules TPM de processeur. Le réseau peut se composer d'un module TPM physique par processeur maître sur des plateformes de gamme d'entrée à moyenne, or de modules TPM redondants via des processeurs maître ou maître de remplacement sur les plateformes d'entreprise multinoeuds. Le microprogramme de la chaîne de confiance enregistre également tous les événements de manière appropriée dans des journaux d'événements TPM.

L'attestation prend en charge l'amorçage digne de confiance conforme à Trusted Computing Group (TCG) 2.0. L'infrastructure TPM prend en charge l'implémentation d'une attestation à distance de référence dont la source est ouverte par IBM.

Le module TPM du processeur hôte est préparé pour l'attestation à distance dans l'industrie de transformation et inclut une phase d'application des accès et une phase d'initialisation. L'*application des accès TPM* est un processus unique, effectué sur les unités remplaçable en clientèle du module TPM avant l'assemblage du système. L'*application des accès TPM* prépare le module TPM à fournir les services de sécurité nécessaires à ses utilisateurs de pile complète. L'*application des accès TPM* inclut la définition de valeurs de préconfiguration TPM, de valeurs et politiques d'autorisation, de hiérarchies de mise à disposition et l'installation de certificats et clés appropriés dans l'espace rémanent TPM, afin de lier les certificats au module TPM spécifié. Ce processus inclut l'établissement d'un certificat de plateforme et clé d'adhésion pour les systèmes à un seul noeud, et d'un certificat de noeud pour les systèmes multinoeuds. A ce stade du traitement, le système requiert une certification d'un autorité de certification IBM.

L'*initialisation TPM* est effectuée par le microprogramme une fois par IPL. Le module TPM effectue ensuite une transition d'un état hors tension (réinitialisation déclarée ou mise sous tension TPM non appliquée) à un état initialisé. L'*initialisation TPM* inclut la réinitialisation de Roots of Trust for Measurement, la validation du microprogramme TPM, ainsi que la préparation à l'acceptation de commandes sur l'interface TPM. L'autotest TPM (extension comme définie par le principe de démarrage de plateforme) est effectué avant que le module TPM passe à l'état pleinement opérationnel.

Mise à disposition de TPM 2.0

Processus de mise à disposition du module TPM (Trusted Platform Module).

Le processus de *mise à disposition de TPM* dans l'industrie de transformation implique les exigences suivantes :

- Des modules TPM doivent être disponibles sur des cartes connectables pour toutes les plateformes POWER9. Cette exigence permet de fournir un point de contrôle unique à la *mise à disposition de TPM*. La *mise à disposition de TPM* est conçue à partir du traitement des données techniques essentielles/de la carte d'ancrage POWER7/POWER8.

- La *mise à disposition de TPM* doit être effectuée via un processus de sous-assemblage hors ligne (et non le processus de chaîne d'assemblage de sous-système de stockage MFG).
- Une fois la *mise à disposition de TPM* effectuée, la carte de module TPM est toujours considérée comme une carte générique qui ne possède pas d'informations spécifiques d'ordre ou de système.
- Une fois la carte TPM mise à disposition, elle devient un composant APC3 (Asset Protection Classification number 3, classification de protection des actifs de niveau 3, tel que défini dans le suivi de la chaîne d'approvisionnement sécurisée).
- La *mise à disposition de TPM* requiert la connectivité à une autorité de certification IBM lors de la mise à disposition de la carte TPM.
- La *mise à disposition de TPM* requiert un processus de restauration de la carte TPM à un état expédiable en cas d'annulation de distribution.

Journaux des événements TPM

Lors de l'exécution d'une opération d'extension du registre de configuration de plateforme (PCR) du module TPM (Trusted Platform Module), une entrée de journal des événements est enregistrée dans le fichier journal des événements TPM. Ce fichier journal est utilisé par des entités externes qui dépendent de l'attestation à distance et par le microprogramme hôte durant la synchronisation multinoeuds. Les fichiers journaux sont utilisés pour reconstruire et valider les valeurs PCR en fonction de valeurs connues. Les fichiers journaux des événements ne sont pas conservés par le module TPM. C'est pourquoi le microprogramme doit fournit le stockage pour les fichiers journaux, ainsi que des interfaces pour mettre à jour les fichiers journaux sur les extensions PCR et accéder aux fichiers journaux à des fins d'attestation.

Parce que les opérations initiales d'*extension PCR* sont effectuées par le code HB (Host Boot), quand POWER Hypervisor (PHYP) est démarré, les informations du journal des événements qui sont associées aux opérations d'extension de la durée d'IPL (procédure de chargement initial) sont sauvegardées dans le code HB. Ce code communique également les entrées de journal d'événements à PHYP via la structure de zone de données hôte (HDAT).

L'hyperviseur PHYP conserve les informations du journal des événements TPM à l'état d'adjoint TPM physique (pTPM). Un maximum de 64 Mo de zone de stockage est allouée à chaque fichier journal TPM. La préférence est donnée aux entrées de journal créées pour des mises à jour de microprogramme simultanées (également appelées entrées de journal non liées). Les plateformes d'entrée de gamme et de gamme moyenne possèdent un pTPM unique par noeud. Les plateformes d'entreprise multinoeuds disposent d'un autre pTPM (redondant) par noeud.

si un tampon de consignation TPM est plein, des opérations d'*extension PCR* supplémentaires pour le module TPM sont autorisées. La troncature du fichier journal est enregistrée et les interfaces d'attestation reçoivent un indicateur signalant que les fichiers journaux distribués ont été tronqués.

Au moment de l'IPL, des opérations d'*extension PCR* avec les informations de journal des événements appropriées sont créées. Des opérations d'*extension PCR* sont également créées pour les mises à jour de microprogramme simultanées. Les fichiers journaux incluent des mesures de code et l'historique de plateforme et de configuration.

Une estimation actuelle pour un premier IPL (à froid) donne 50 enregistrements d'événement par noeud sur un système à noeud unique, et 200 enregistrements d'événement par noeud sur un système à quatre noeuds (à 128 octets par enregistrement, ce débit est de 25 Ko par noeud par IPL).

Les informations du journal des événements TPM peuvent être obtenues via un cliché de ressource. Les fichiers journaux d'événements ne sont PAS migrés avec les partitions logiques car les fichiers journaux sont associés à la plateforme physique. De ce fait, l'historique TPM des modules TPM physiques peut différer de l'historique TPM des partitions logiques.

Les paramètres de configuration TPM qui ne nécessitent pas de noeud TPM lors d'un premier IPL (à froid) ou d'IPL suivants (à chaud) n'ont ps besoin des fichiers journaux d'événements. Toutefois, si l'option **TPM requis** est défini, les opérations d'*extension PCR* et les fichiers journaux associés doivent être conservés.

Signatures et clés dans le cadre de l'amorçage sécurisé

La conception de la sécurité utilise des clés asymétriques et le hachage des clés publiques matériel est stocké dans la mémoire morte Serial Electrically Erasable Programmable ROM (SEEPROM). Le code de vérification provenant de la mémoire SEEPROM, ainsi que les clés publiques matériel et ds clés publiques logiciel supplémentaires, est utilisé pour valider les signatures de ces images de code du microprogramme dans les conteneurs de code. Chaque image de microprogramme qui doit s'exécuter sur les processeurs coeur est chargée dans la mémoire système sous forme de conteneur de code, incluant un en-tête de préfixe avec les informations de sécurité nécessaires et l'image du code. Le processus de validation de conteneur garantit l'intégrité du code (i.e. le code reste inchangé) et l'authentification du code (i.e. signé par l'autorité appropriée).

Les clés privées de signature du code sont stockées dans un matériel sécurisé (par exemple, IBM 4767 Cryptographic Coprocessor), derrière un pare-feu avec un accès restreint et des contrôles d'audit complets.

Attestation à distance du logiciel système

Le module TPM (Trusted Platform Module) permet l'attestation à distance de la pile de code sur un système en cours d'exécution. Le microprogramme de la chaîne de confiance enregistre le hachage du microprogramme chargé et stocke les enregistrements sur le réseau des modules TPM Amorçage sécurisé. Le réseau peut comporter un module TPM physique par processeur maître sur des plateformes processeur POWER9. L'attestation prend en charge l'amorçage digne de confiance conforme à Trusted Computing Group (TCG) 2.0. L'infrastructure TPM identifiée prend en charge les piles d'attestations futures.

Les interfaces d'attestation physique autorisent un client tiers de confiance à extraire des informations sur l'état d'amorçage sécurisé du système PowerVM cible. Ce processus utilise les modules TPM physiques qui sont des unité conforme à TCG 2.0. Ces modules sont utilisés par le microprogramme du système pour étendre des mesures durant le processus d'amorçage.

Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même le fonctionnement des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevets. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
U.S.A.

Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations
IBM Canada Ltd
3600 Steeles Avenue East
Markham, Ontario
L3R 9Z7 Canada

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues par écrit à l'adresse suivante :

Intellectual Property Licensing
Legal and Intellectual
Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT. IBM DECLINE TOUTE RESPONSABILITE, EXPLICITE OU IMPLICITE, RELATIVE AUX INFORMATIONS QUI Y SONT CONTENUES, Y COMPRIS EN CE QUI CONCERNE LES GARANTIES DE NON-CONTREFACON ET D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Il est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
U.S.A.

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions de l'ICA, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performances et les exemples de clients sont fournis à titre d'exemple uniquement. Les performances réelles peuvent varier en fonction des configurations et des conditions d'exploitations spécifiques.

Les informations concernant des produits de fabricants tiers ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits de fabricants tiers doit être adressée aux fournisseurs de ces produits.

Les instructions relatives aux intentions d'IBM pour ses opérations à venir sont susceptibles d'être modifiées ou annulées sans préavis, et doivent être considérées uniquement comme un objectif.

Tous les tarifs indiqués sont les prix de vente actuels suggérés par IBM et sont susceptibles d'être modifiés sans préavis. Les tarifs appliqués peuvent varier selon les revendeurs.

Ces informations sont fournies uniquement à titre de planification. Elles sont susceptibles d'être modifiées avant la mise à disposition des produits décrits.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes ou de sociétés serait purement fortuite.

LICENCE DE COPYRIGHT :

Le présent logiciel contient des exemples de programmes d'application en langage source destinés à illustrer les techniques de programmation sur différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquels ils ont été écrits ou aux interfaces de programmation IBM. Ces exemples de programmes n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes. Les exemples de programmes sont fournis "EN L'ETAT", sans garantie d'aucune sorte. IBM ne sera en aucun cas responsable des dommages liés à leur utilisation.

Toute copie totale ou partielle de ces programmes exemples et des oeuvres qui en sont dérivées doit comprendre une notice de copyright, libellée comme suit :

© (nom de votre entreprise) (année).
Des segments de code
sont dérivés des Programmes exemples d'IBM Corp.
© Copyright IBM Corp.
entrez l'année ou les années.

Si vous visualisez ces informations en ligne, il se peut que les photographies et illustrations en couleur n'apparaissent pas à l'écran.

Fonctions d'accessibilité pour les serveurs IBM Power Systems

Les fonctions d'accessibilité aident les utilisateurs souffrant d'un handicap tel qu'une mobilité réduite ou une vision limitée à utiliser la technologie de l'information.

Présentation

Les serveurs IBM Power Systems incluent les fonctions d'accessibilité principales suivantes :

- Fonctionnement uniquement au clavier
- Opérations utilisant un lecteur d'écran

Les serveurs IBM Power Systems utilisent la dernière norme W3C, WAI-ARIA 1.0 (www.w3.org/TR/wai-aria/), afin de garantir la conformité à la US Section 508 (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) et au Web Content Accessibility Guidelines (WCAG) 2.0 (www.w3.org/TR/WCAG20/). Pour tirer parti des fonctions d'accessibilité, utilisez l'édition la plus récente de votre lecteur d'écran et le tout dernier navigateur Web pris en charge par les serveurs IBM Power Systems.

La documentation produit en ligne des serveurs IBM Power Systems dans l'IBM Knowledge Center est activée pour l'accessibilité. Les fonctions d'accessibilité de l'IBM Knowledge Center sont décrites à la section Accessibility de l'aide sur l'IBM Knowledge Center (www.ibm.com/support/knowledgecenter/doc/kc_help.html#accessibility).

Navigation au clavier

Ce produit utilise les touches de navigation standard.

Informations sur l'interface

Les interfaces utilisateur des serveurs IBM Power Systems ne comportent pas de contenu clignotant 2 à 55 fois par seconde.

L'interface utilisateur Web des serveurs IBM Power Systems est basée sur des feuilles de style en cascade afin de rendre de manière approprié le contenu et de fournir une expérience fiable. L'application fournit un moyen équivalent pour les utilisateurs ayant une mauvaise vue d'utiliser les paramètres d'affichage du système, y compris le mode contraste élevé. Vous pouvez contrôler la taille de police à l'aide des paramètres d'unité ou de navigateur Web.

L'interface utilisateur Web des serveurs IBM Power Systems inclut des repères de navigation WAI-ARIA utilisables pour rapidement accéder à des zones fonctionnelles de l'application.

Logiciel du fournisseur

Les serveurs IBM Power Systems sont fournis avec différents logiciels fournisseur qui ne sont pas couverts par le contrat de licence IBM. IBM ne garantit en aucune façon les fonctions d'accessibilité desdits produits. Contactez le fournisseur afin d'obtenir les informations d'accessibilité relatives à ces produits.

Informations d'accessibilité connexes

Outre les sites Web du support et du centre d'assistance IBM, IBM propose un service de téléphone par téléscripteur à l'usage des clients sourds ou malentendants leur permettant d'accéder aux services des ventes et du support :

Service de téléscripteur
800-IBM-3383 (800-426-3383)
(Amérique du Nord)

Pour plus d'informations sur l'engagement d'IBM concernant l'accessibilité, voir IBM Accessibility (www.ibm.com/able).

Politique de confidentialité

Les Logiciels IBM, y compris les Logiciels sous forme de services ("Offres Logiciels") peuvent utiliser des cookies ou d'autres technologies pour collecter des informations sur l'utilisation des produits, améliorer l'acquis utilisateur, personnaliser les interactions avec celui-ci, ou dans d'autres buts. Bien souvent, aucune information personnelle identifiable n'est collectée par les Offres Logiciels. Certaines Offres Logiciels vous permettent cependant de le faire. Si la présente Offre Logiciels utilise des cookies pour collecter des informations personnelles identifiables, des informations spécifiques sur cette utilisation sont fournies ci-dessous.

Cette Offre Logiciels n'utilise pas de cookies ou d'autres techniques pour collecter des informations personnelles identifiables.

Si les configurations déployées de cette Offre Logiciels vous permettent, en tant que client, de collecter des informations permettant d'identifier les utilisateurs par l'intermédiaire de cookies ou par d'autres techniques, vous devez solliciter un avis juridique sur la réglementation applicable à ce type de collecte, notamment en termes d'information et de consentement.

Pour plus d'informations sur l'utilisation à ces fins des différentes technologies, y compris les cookies, consultez les Points principaux de la Déclaration IBM de confidentialité (http://www.ibm.com/privacy/fr/fr), la Déclaration IBM de confidentialité sur Internet (http://www.ibm.com/privacy/details/fr/fr), notamment la section "Cookies, pixels espions et autres technologies", ainsi que la page "IBM Software Products and Software-as-a-Service Privacy Statement" (http://www.ibm.com/software/info/product-privacy), disponible en anglais uniquement.

Informations relative à l'interface de programmation

Cet amorçage sécurisé dans les publications PowerVM est destiné aux interfaces de programmation permettant au client d'écrire des programmes afin d'obtenir les services d'IBM AIX version 7.2, IBM AIX version 7.1, IBM AIX version 6.1, IBM i 7.4 et IBM Virtual I/O Server version 3.1.1.

Marques

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corp. dans de nombreux pays. Les autres noms de produits et de services peuvent être des marques d'IBM ou d'autres sociétés. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web Copyright and trademark information.

Dispositions

Les droits d'utilisation relatifs à ces publications sont soumis aux dispositions suivantes.

Applicabilité : Les présentes dispositions s'ajoutent aux conditions d'utilisation du site Web IBM.

Usage personnel : Vous pouvez reproduire ces publications pour votre usage personnel, non commercial, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez distribuer ou publier tout ou partie de ces publications ou en faire des oeuvres dérivées sans le consentement exprès d'IBM.

Usage commercial : Vous pouvez reproduire, distribuer et afficher ces publications uniquement au sein de votre entreprise, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez reproduire, distribuer, afficher ou publier tout ou partie de ces publications en dehors de votre entreprise, ou en faire des oeuvres dérivées, sans le consentement exprès d'IBM.

Droits : Excepté les droits d'utilisation expressément accordés dans ce document, aucun autre droit, licence ou autorisation, implicite ou explicite, n'est accordé pour ces publications ou autres informations, données, logiciels ou droits de propriété intellectuelle contenus dans ces publications.

IBM se réserve le droit de retirer les autorisations accordées ici si, à sa discrétion, l'utilisation des publications s'avère préjudiciable à ses intérêts ou que, selon son appréciation, les instructions susmentionnées n'ont pas été respectées.

Vous ne pouvez télécharger, exporter ou réexporter ces informations qu'en total accord avec toutes les lois et règlements applicables dans votre pays, y compris les lois et règlements américains relatifs à l'exportation.

IBM NE DONNE AUCUNE GARANTIE SUR LE CONTENU DE CES PUBLICATIONS. LES PUBLICATIONS SONT LIVREES EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. LE FABRICANT DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.