Power Systems

Arranque seguro en PowerVM

Power Systems

Arranque seguro en PowerVM

Nota

Antes de utilizar esta información y el producto al que da soporte, lea la información incluida en el apartado “Avisos” en la página 11.

Esta edición se aplica a to IBM AIX Versión 7.2, a IBM AIX Versión 7.1, a IBM AIX Versión 6.1, a IBM i 7.3 (número de producto 5770-SS1), al Servidor de E/S virtual de IBM versión 3.1.0.0 y a todos los releases y modificaciones posteriores hasta que se indique lo contrario en nuevas ediciones. Esta versión no funciona en todos los modelos RISC (Reduced Instruction Set Computer) ni tampoco en los modelos CISC.

Contenido

Arranque seguro en PowerVM

Los servidores IBM® Power Systems proporcionan una plataforma de servidor altamente segura. El hardware y firmware basado en procesadores de IBM POWER9 incluyen nuevas características de PowerVM para proporcionar una plataforma más segura para el despliegue en la nube.

Las características clave de PowerVM disponibles en servidores basados en procesadores POWER9 incluyen:

- Un proceso de carga de programa inicial segura (IPL) o la característica Arranque seguro solo permite que se ejecuten en los procesadores del sistema componentes de firmware firmados oportunamente. Cada componente de la pila de firmware, incluido arranque de host, el hipervisor POWER (PHYP) y el firmware de partición (PFW), tiene la firma del fabricante de plataformas y está verificado como parte del proceso de IPL.
- Una infraestructura que dé soporte a la certificación remota de la pila de firmware del sistema a través de un módulo de plataforma de confianza (TPM) de hardware.

Arranque seguro y arranque de confianza

Para esta documentación, los términos *Arranque seguro* y *Arranque de confianza* tienen connotaciones específicas. Los términos se utilizan como conceptos distintos pero complementarios a la vez.

Arranque seguro
: La característica Arranque seguro protege la integridad del sistema utilizando firmas digitales para realizar verificación protegida mediante hardware de todos los componentes de firmware. También distingue entre el dominio de confianza del sistema de host y el dominio de confianza del procesador de servicio flexible (FSP), controlando el acceso de la interfaz de servicio y del procesador de servicio a regiones de memoria sensibles del sistema.

Arranque de confianza
: La característica de arranque de confianza crea mediciones de plataformas protegidas y fuertes desde el punto de vista criptográfico que prueban que determinados componentes de firmware se han ejecutado en el sistema. Puede evaluar las mediciones utilizando protocolos fiables para determinar el estado del sistema y utilizar dicha información para decisiones relativas a la seguridad.

Novedades del arranque seguro en PowerVM

Lea detenidamente las novedades o los cambios realizados en el arranque seguro en PowerVM desde la última actualización de esta recopilación de temas.

Agosto de 2018

- En esta recopilación de temas se han llevado a cabo diversas actualizaciones.

Términos

Aprenda los términos que se utilizan en esta documentación.

Adjunto
: Una partición hija que utiliza CPU asignada a otra partición. Un adjunto está fácilmente disponible para el administrador del sistema y se puede utilizar para prestar servicio a la partición principal.

Unidad de modificación/visualización (ADU)
Recurso de hardware que se utiliza para acceder al almacenamiento principal. Una ADU la utilizan los elementos de hardware y de firmware.

Contenedor de código
Imagen de código verificable que tiene una cabecera de prefijo Arranque seguro. El contenedor es una estructura que consta de una cabecera de 4K (cabecera de hardware o cabecera de firmware), seguida de una carga útil protegida (una imagen de código que tiene un hash en la cabecera de prefijo) y cualquier dato de carga útil que sea exclusiva del servidor.

Autorización para firma de código
El nivel de autorización que se otorga a personas con conocimientos del código de asunto para permitir cumplir un rol como firmante autorizado para firmar funciones de servidor.

Raíz base de confianza para mediciones (CRTM)
Un código de confianza prioritario (inmutable) que forma parte de la credencial de la plataforma. En el modelo RTM estático, el código CRTM se debe ejecutar primero cuando el entorno de hardware físico o del servidor está encendido o cuando el entorno de hardware físico o del servidor se ha restablecido. Para la característica de Arranque seguro, el código CRTM está basado en el motor autoarranque/arranque de host (SBE/HB). El código CRTM incluye el motor de autoarranque y el código de arranque de host suficiente para permitir que se inicialice un controlador de dispositivo TPM.

Management Console (MC)
Una interfaz para que los administradores del sistema y los representantes de servicio vean y realicen tareas relativas al particionamiento de hardware y aspectos de servicio de un sistema.

Procesador maestro
Procesador en el nodo que está conectado físicamente a la memoria flash No O (NOR).

Ampliación PCR
Una operación que se realiza en los registros de la configuración de la plataforma TPM (PCR) para actualizar el valor del registro para registrar el historial de mensajes que se amplían al registro. En lugar de realizar la operación de escritura directamente en un PCR, la operación de ampliación PCR tiene el valor original en el PCR, concatena el nuevo mensaje a éste y toma un hash para producir un valor de registro actualizado. El historial de mensajes que se amplía y el orden de las ampliaciones se puede comparar más adelante con los registros de sucesos TPM correspondientes.

Certificado de plataforma
Certifica que existe en el TPM, que certifica que la plataforma asociada TPM sea una plataforma de IBM con un código CRTM. El certificado no depende del modelo de plataforma.

PNOR Procesador no-OR (PNOR), también conocido como flash.

Cabecera de prefijo
Una estructura de 4 KB cuyo prefijo son imágenes de código firmado de contenedores de código Arranque seguro.

Clave privada para firma de código
Parte privada o secreta de un par de claves pública/privada que se utiliza para criptografía de clave pública, utilizando algoritmos de clave asimétrica.

Registros protegidos
Registros que son de solo lectura utilizando comunicación de exploración (SCOM) mediante procesador de servicio flexible (FSP) pero son de lectura/escritura utilizando código de confianza. En la mayoría de los casos, estos registros son independientes del valor que se explora en la inicialización y toman el valor predeterminado de un valor conocido.

Clave pública para firma de código
Parte pública o publicada de un par de claves pública/privada que se utiliza para criptografía de clave pública, utilizando algoritmos de clave asimétrica.

Certificación remota
Comprueba qué software se ejecuta en un sistema remoto. La certificación es el proceso de validar la precisión de la información. La certificación remota permite que las partes interesadas autorizadas determinen cambios en el sistema del usuario, comprobando el estado de TPM y de la plataforma en la que reside.

Motor de auto arranque (SBE)
Es el motor de reinicialización de arranque que se utiliza para inicializar el chip del procesador para ejecutar los procedimientos de arranque de host.

Firma Demuestra la autenticidad de un mensaje. La firma consta del hash del mensaje de asunto que está cifrado con la mitad de un par de claves pública/privada.

Raíz estática de confianza para mediciones (SRTM)
Un sistema arranca desde una parte inmutable del código de firmware que se presupone que es de confianza en todo momento. La acción de arranque inicia el proceso de mediciones, en el que cada componente mide el siguiente componente en una cadena.

Bloques de construcción de confianza (TBB)
Incluye las partes de las raíces de confianza para mediciones (RTM) que no tienen ubicaciones protegidas o prestaciones protegidas. TBB incluye la CRTM, conexión del almacenamiento de CRTM a una placa del sistema, la conexión de TPM a una placa del sistema y mecanismos para determinar presencia física del usuario.

Código de confianza
Firmware que autoriza autoridades de hardware y firmware de IBM previamente designadas. La fuente del código se autentica y se comprueba la integridad de la imagen.

Trusted Computing Group (TCG)
Trusted Computing Group es la organización sin ánimo de lucro que se formó para desarrollar, definir y promover estándares del sector abiertos, neutros respecto del proveedor y globales, que da soporte a una raíz de confianza para mediciones (RTM) basada en hardware para plataformas informáticas interoperables de confianza.

Memoria de confianza
Región de la memoria que solo es accesible (lectura y escritura) mediante código de confianza. El acceso a la memoria de confianza está bloqueado por mecanismos de aislamiento de hardware cuando el sistema arranca en modalidad segura. Una pequeña sección de la memoria que se encuentra fuera de la región de memoria de confianza se conoce como *memoria sin confianza* y puede ser fácilmente accesible por interfaces de servicio para realizar operaciones de lectura y escritura.

Módulo de plataforma fiable (TPM)
Coprocesador criptográfico de bajo rendimiento parecido a una tarjeta inteligente. Un TPM puede almacenar hashes de la secuencia de arranque en un conjunto de registros de configuración de plataforma (PCR).

Memoria no de confianza
La región de memoria con acceso abierto de lectura y escritura que incluye procesador de servicio flexible (FSP) e interfaces de servicio que existen fuera del dominio de seguridad de los procesadores host.

Validación
Verifique la identidad del firmante, por ejemplo, la validación de un contenedor de código significa verificar que el código en la imagen contenida lo firme de forma digital IBM y que la imagen no se modifique.

Código de verificación
El código protegido existe en la memoria de solo lectura programable y borrable eléctricamente (SEEPROM) y proporciona el soporte de verificación de firma para los contenedores de código de

arranque seguro. El código de verificación es el elemento clave que se utiliza para establecer la raíz base de confianza para mediciones durante el arranque seguro.

Proceso seguro de la carga del programa inicial (IPL)

La característica Arranque seguro impide el acceso no autorizado a datos del cliente a través de firmware no autorizado que se ejecuta en un procesador del sistema o accediendo a través de las vulnerabilidades de seguridad en un firmware de procesador de servicio autorizado o a través de interfaces de servicio de hardware a las que se accede a través del procesador de servicio flexible (FSP).

Mientras que la característica Arranque seguro impide el acceso no autorizado a datos del cliente, los mecanismos de Arranque seguro no proporcionan protección contra las amenazas siguientes:

- Ataques basados en software del sistema operativo para obtener acceso no autorizado a datos del cliente.
- Administradores de sistemas fraudulentos
- Ataques físicos de hardware (por ejemplo, sustituciones de chips y registro de tráfico de bus).

La característica Arranque seguro implementa una cadena de confianza basada en el procesador en el hardware del procesador de POWER9 que ha habilitado la pila de firmware de POWER9. La característica Arranque seguro proporciona una base de firmware de confianza para mejorar la confidencialidad y la integridad de los datos de clientes en un entorno virtualizado.

La característica de arranque de confianza de servidores basados en procesadores POWER9 permite la medición del código de vía de acceso de configuración del sistema y de carga del programa inicial (IPL), que se pueden utilizar más adelante como prueba, mediante certificación de la configuración de la vía de acceso IPL inicial del sistema. Para crear una raíz básica de confianza para estas mediciones (CRTM), se utiliza un flujo Arranque seguro que añade comprobaciones criptográficas en cada fase del proceso de IPL hasta que se establece la comunicación con el módulo de plataforma fiable (TPM). El flujo Arranque seguro garantiza la integridad de todo el firmware que se debe ejecutar en procesadores de núcleo, lo que impide que se ejecute cualquier firmware modificado de forma maliciosa o no autorizada. Una anomalía para autenticar el código en cualquier punto impide que el proceso de IPL acabe completándose.

La característica Arranque seguro en sistemas POWER9 establece la confianza a través del proceso de arranque de plataforma. Aquí, *de confianza* significa que el código que se ejecuta durante el proceso de IPL se origina desde el fabricante de plataformas, tiene la firma del fabricante de plataformas y no se ha modificado.

La protección de modalidad segura disponible en servidores basados en procesadores POWER9 mantiene la confianza, impidiendo el acceso de lectura/escritura a los datos del cliente mediante interfaces FSP y de servicio, impidiendo la ejecución de código no de confianza en el procesador de host y manteniendo la confianza en todos los puntos clave en el proceso Arranque seguro.

La característica de POWER9 de Arranque seguro implementa una cadena de confianza basada en un procesador. La cadena se inicia con un componente de confianza implícitamente, mientras los demás componentes se autentican y se comprueba su integridad antes de que se ejecuten en núcleos de procesadores de host. El código de verificación que se encuentra en el procesador bloqueado en ROM programable y borrable eléctricamente en serie (SEEPROM) valida la carga de firmware inicial. El firmware verifica las firmas criptográficas de todo el firmware posterior que debe ser de confianza y que debe cargarse para su ejecución en los núcleos del procesador POWER9. En un sistema POWER9, los conmutadores de seguridad SEEPROM están establecidos en el código de motor de autoarranque (SBE) y se arreglan en la línea de ensamblaje de fabricación (MFG) del sistema para proporcionar la base para el cumplimiento de hardware de flujos IPL seguros. Los puentes de modalidad de seguridad física están disponibles en la *placa posterior* de un sistema. Los puentes se pueden utilizar para alterar temporalmente los conmutadores de modalidad segura del procesador si una persona accede físicamente al sistema. El proceso de IPL seguro mejora más la informática de confianza en la plataforma de Power.

El diagrama siguiente ilustra las operaciones de un proceso de IPL de arranque seguro y de confianza.

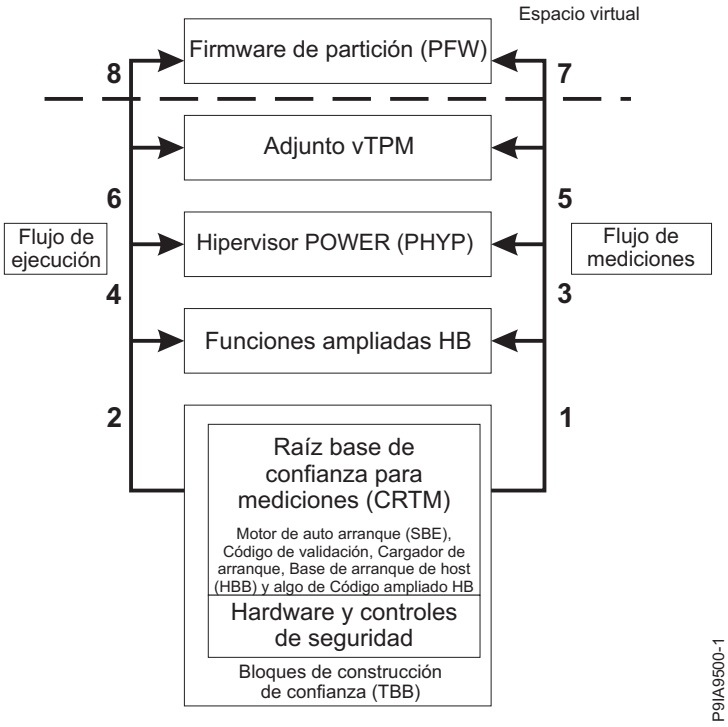

Figura 1. Flujo de arranque seguro y de confianza

La característica Arranque seguro establece el código base de SEEPROM, SBE bloqueados y el código base de arranque de host (incluida una pequeña parte de código ampliado de arranque de host) como raíz base de confianza para mediciones (CRTM), con la cadena de confianza ampliada que incluya POWER Hypervisor (PHYP), firmware de partición (PFW), particiones de adjuntos seleccionados (módulo de plataforma fiable físico (pTPM), módulo de plataforma fiable virtual (vTPM), tiempo de ejecución de arranque de host y adjuntos de cifrado) y controlador en chip (OCC – gestión térmica). Este dominio fiable y el soporte de seguridad de hardware del procesador garantizan que los datos del cliente no se visualicen o se alteren a través de ningún mecanismo de hardware o firmware.

La pila de firmware de confianza completa se autentica utilizando imágenes firmadas y se ejecuta en ubicaciones de memoria de confianza. El FSP se mantiene fuera del dominio de confianza del servidor host y el FSP queda bloqueado del acceso a registros de la unidad de dirección/visualización (ADU), otros registros protegidos y regiones de memoria de confianza. El motor de autoarranque (SBE) aplica el bloqueo FSP filtrando la lista negra de recursos de comunicación de exploración de lectura/escritura de registro de procesador. Los recursos SCOM están habilitados por el conmutador de acceso seguro en el área SEEPROM del chip del procesador.

La figura siguiente muestra el entorno de Arranque seguro.

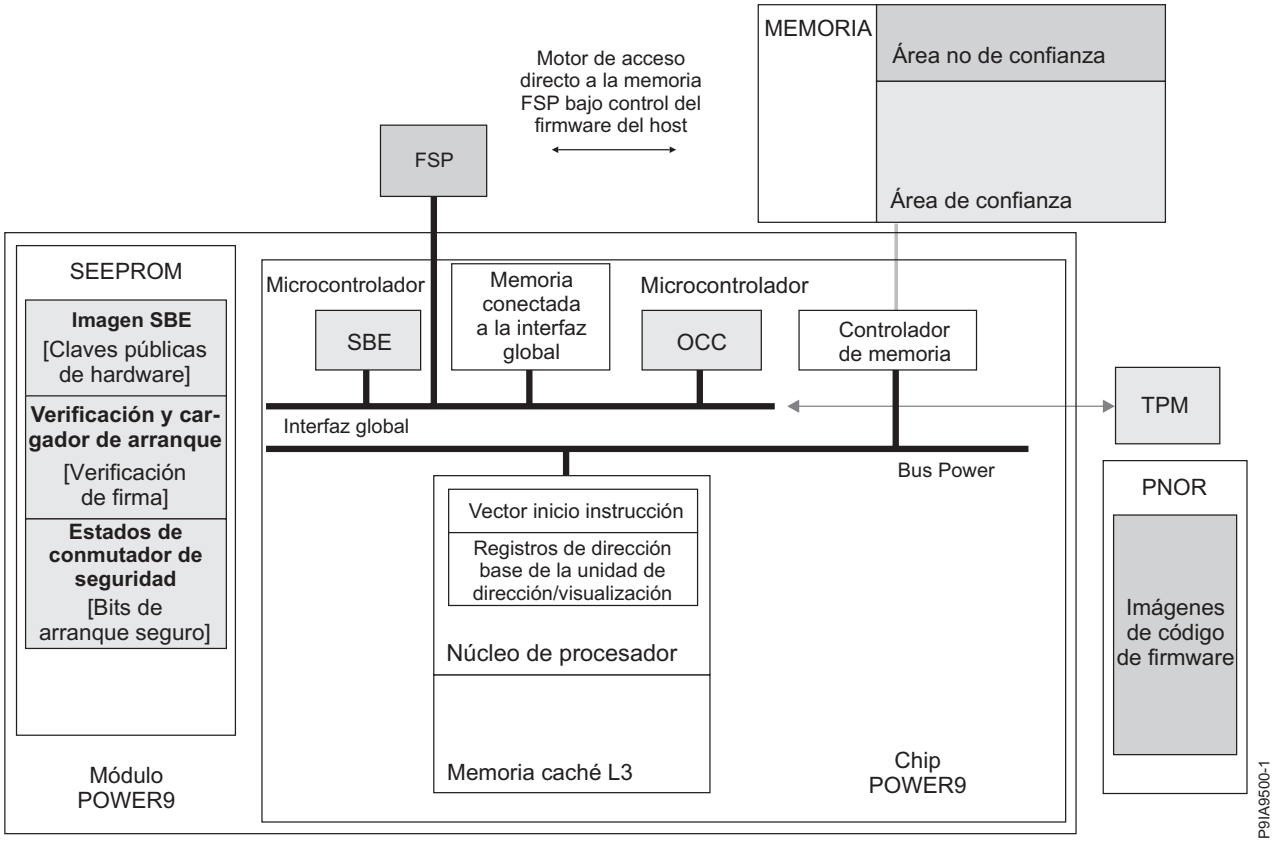

Figura 2. El entorno de Arranque seguro

Cuando se inicia el proceso Arranque seguro, el elemento FSP envía una solicitud de arranque y detalles sobre el tipo de arranque a chips de procesador en el sistema. Internamente, en el estado de la lógica de Arranque seguro se borran los valores establecidos previamente para iniciarse con un estado adecuado y conocido. En el estado también se borra cualquier solicitud de atenuación que se hubiera ejecutado anteriormente. Se implementan mecanismos de protección de hardware para impedir que un atacante malicioso se salte este paso inicial. El acceso desde el FSP a recursos de chip internos está bloqueado y el motor Arranque seguro empieza a captar código de inicialización de la memoria que está en el módulo, seguro, no volátil y bloqueado. Este código realiza inicialización de chip básico y restablece el TPM.

Después de que se haya completado el paso inicial en el proceso de arranque, el motor de autoarranque (SBE) carga el cargador de arranque de host y el código de validación de SEEPROM en la memoria caché L3 interna del chip del procesador. A continuación, se inicia un núcleo del procesador y el cargador de arranque capta el código Base de arranque de host (HBB) inicial del chip flash de NOR de procesador (PNOR) y lo carga en la memoria caché L3. En modalidad segura, el código de validación de la memoria caché L3 se utiliza para verificar la imagen HBB que está ahora disponible en la memoria caché de confianza. Tras verificar el código flash inicial, el núcleo de procesador continúa ejecutando el código validado del espacio de memoria de confianza y carga y valida las funciones ampliadas HB (HBI). Después de que se mida el HBI y se verifique y se copie, su medición (hash de imagen), que indica la autenticación válida, se registra en el TPM, tal como lo indica el **Paso 1** en la Figura Flujo de arranque seguro y de confianza. En este punto, todo el código que se ejecuta está plenamente contenido en el chip flash PNOR y el sistema no se ha accedido por ningún otro mecanismo. Esto se conoce como el límite del arranque de confianza. En caso de que la verificación falle, el sistema se detiene inmediatamente y está protegido mediante mecanismos de protección de hardware para impedir la ejecución de código no fiable o fraudulento.

A continuación, el código HB gestiona las actualizaciones pendientes de la memoria no volátil segura utilizando una nueva imagen de confianza. Para proteger la raíz de base de confianza (CRTM), el código HB bloquea la memoria segura, impidiendo así cualquier acceso posterior de escritura a la memoria (esta acción significa que si el sistema se vuelve a arrancar, vuelve al estado de confianza). A continuación, el código HB inicializa el controlador de memoria en chip y los módulos de memoria en línea duales conectados (DIMMs). El código HB también inicializa otros chips que están directamente conectados al procesador en el que se ejecuta antes de establecer la interfaz coherente de memoria a otros chips del sistema. Estos otros chips también se verifican para garantizar que tienen un estado seguro y de confianza.

A continuación los componentes de pila de firmware superiores se cargan, verifican, ejecutan y sus mediciones se registran en el TPM. Esta acción completa el **Paso 2**, que se indican en la Figura Flujo de arranque seguro y de confianza. En el **Paso 3** de la figura Flujo de arranque seguro y de confianza, la carga útil de POWER Hypervisor (PHYP) se carga en la memoria principal. A continuación, el código se autentica de forma criptográfica y tras una autenticación con éxito, PHYP empieza a ejecutarse. La medición de autenticación del código PHYP se registra en el TPM. Asimismo, los **pasos 4 a 8**, que se indican en la Figura Flujo de arranque seguro y de confianza se realizan para cargar el código de la memoria flash no bloqueada, el código se autentica de forma criptográfica y, a continuación, se ejecutan varios adjuntos y el firmware de partición (PFW).

Soporte TPM físico en arranque seguro

El módulo de plataforma fiable (TPM) permite la certificación remota de la pila de código en un sistema en ejecución. La cadena de firmware de confianza registra el hash del firmware cargado y almacena los registros en la red de los TPM del procesador. La red consta de un TPM físico por procesador maestro en plataformas de gama baja a media o TPM redundantes a través de plataformas empresariales de múltiples nodos o procesadores maestros alternativos. La cadena de firmware de confianza también registra todos los sucesos correctamente en los registros de sucesos TPM.

La certificación da soporte al arranque de confianza compatible con Trusted Computing Group (TCG) 2.0. La infraestructura TPM da soporte a una implementación de certificación remota de referencia de código abierto de IBM.

El TPM de procesador host está preparado para certificación remota en el sector de fabricación (MFG) e incluye una fase de suministro y una fase de inicialización. *Suministro de TPM* es un proceso único y se realiza en la unidad sustituible localmente (FRU) del módulo TPM antes de ensamblar el sistema. *Suministro de TPM* prepara el TPM para proporcionar los servicios de seguridad necesarios a sus usuarios de pila completa. *Suministro de TPM* incluye establecer valores de preconfiguración TPM, valores y políticas de autorización, jerarquías de suministro e instalación de certificados y claves relevantes en el espacio no volátil TPM (NV), para enlazar los certificados con el TPM especificado. Este proceso incluye establecer una clave de aprobación y un certificado de plataforma para sistemas de nodo único y un certificado de nodo para sistemas de múltiples nodos. En esta etapa del proceso, el sistema requiere una certificación por parte de una entidad emisora de certificados de IBM.

La *inicialización de TPM* la realiza el firmware una vez por carga de programa inicial (IPL). A continuación, el TPM inicia la transición desde un estado de apagado (no se aplica el restablecimiento afirmado o la alimentación TPM) hasta un estado inicializado. La *Inicialización de TPM* incluye restablecer la raíces de confianza para mediciones, la validación de firmware TPM y la preparación para aceptar mandatos en la interfaz TPM. La autoprueba de TPM (ampliación tal como la ha definido la política de inicio de la plataforma) se completa antes de que TPM entre en una modalidad plenamente operativa.

Suministro de TPM 2.0

Aprenda el proceso de suministro del Módulo de plataforma fiable (TPM).

El proceso *Suministro TPM* en el sector de fabricación (MFG) tiene los requisitos siguientes:

- Los TPM deben estar disponibles en tarjetas enchufables para todas las plataformas de POWER9. Este requisito proporciona un único punto de control para *Suministro TPM*. El *Suministro TPM* se ha diseñado basándose en el proceso de datos de producto vital (VPD)/tarjeta de anclaje de POWER7/POWER8.
- El *Suministro TPM* se debe realizar a través de un proceso de subensamblaje fuera de línea (no el proceso de línea de ensamblaje de caja MFG).
- Después del *Suministro TPM*, la tarjeta TPM se sigue considerando una tarjeta genérica que no tiene información específica del pedido o del sistema.
- Después de que se haya dispuesto la tarjeta TPM, se convierte en el componente número 3 de clasificación de protección de activos (APC3) (tal como se ha definido en el seguimiento de la cadena de suministro segura).
- El *Suministro TPM* requiere conectividad a una entidad emisora de certificados de IBM a la vez que suministra la tarjeta TPM.
- El *Suministro TPM* requiere un proceso para restaurar la tarjeta TPM a un estado que se pueda enviar.

Registros de sucesos de TPM

Cuando se realiza una operación de ampliación de registro de configuración de plataforma (PCR) de un módulo de plataforma fiable (TPM), se registra un registro de suceso en un archivo de registro de sucesos TPM. Este archivo de registros lo utilizan entidades externas que dependen de la certificación remota y el firmware de host durante la sincronización de varios nodos. Los archivos de registro se utilizan para reconstruir y validar los valores PCR en valores conocidos. Los archivos de registro de sucesos no los mantiene el TPM. Por consiguiente el firmware debe proporcionar almacenamiento para los archivos de registro y proporcionar interfaces para actualizar los archivos de registro en ampliaciones PCR y acceder a los archivos de registro para fines de certificación.

Dado que las operaciones *Ampliación PCR* las realiza el código de arranque de host (HB), cuando se inicia POWER Hypervisor (PHYP), la información de registro de sucesos que está asociada con las operaciones de ampliación de tiempo de la carga del programa inicial (IPL) se guardan en el código HB. El código HB también se comunica con las entradas relevantes del registro de sucesos a PHYP a través de la estructura del área de datos de host (HDAT).

PHYP mantiene la información del registro de sucesos TPM en el estado de adjunto de TPM físico (pTPM). Se asigna un máximo de 64 MB de área de almacenamiento para cada archivo de registro TPM. Se da preferencia a las entradas de registro que se crean para actualizaciones de firmware simultáneas (también conocidas como entradas de registro no limitadas). Las plataformas de gama baja y media tienen un único pTPM por nodo. Las plataformas empresariales de varios nodos tienen otro pTPM (redundante) por nodo.

Si un almacenamiento intermedio de registro TPM está lleno, se permiten operaciones adicionales de *Ampliación PCR* al TPM. El recorte del archivo de registro se registra y las interfaces de certificación reciben un indicador que indica que los archivos de registro entregados se han truncado.

En el momento de la carga del programa inicial (IPL), se crean operaciones *Ampliación PCR* que tienen información adecuada de registro de sucesos. Las operaciones *Ampliación PCR* también se crean para actualizaciones de firmware simultáneas. Los archivos de registro incluyen mediciones de código y configuración e historial de plataforma.

Las estimaciones actuales en un primer IPL (en frío) son 50 registros de sucesos por nodo en un único sistema de nodos y 200 registros de suceso por nodo en un sistema de cuatro nodos (a 128 B por registro de suceso, esta velocidad es de 25 KB por nodo por IPL).

La información de registro de sucesos TPM se puede obtener a través del volcado de recursos. Los archivos de registro de sucesos NO se migran con particiones lógicas porque los archivos de registro

están asociados con la plataforma física. Por consiguiente, es posible que el historial TPM de los TPM físicos (pTPM) no sea el mismo que el historial de TPM de las particiones lógicas.

Los valores de configuración de TPM que no requieren un TPM de nodo durante un primer IPL (en frío) o un IPL (en caliente) posterior no requieren archivos de registro de sucesos. No obstante, si la opción **TPM necesario** está establecida, las operaciones *Ampliación PCR* y los archivos de registro de sucesos asociados se deben mantener.

Firmas y claves en arranque seguro

El diseño de seguridad utiliza claves simétricas y el hash de las claves públicas de hardware se almacenan en la ROM programable y borrable eléctricamente en serie (SEEPROM). El código de verificación de SEEPROM, junto con las claves públicas de hardware y las claves públicas de software adicionales, se utilizan para validar las firmas de las imágenes de código de firmware en los contenedores de código. Cada imagen de firmware que se debe ejecutar en los procesadores núcleo se carga en la memoria del sistema como contenedor de código, incluida una cabecera de prefijo con la información de seguridad necesaria y la imagen de código. El proceso de validación del contenedor garantiza la integridad del código (es decir, el código permanece sin modificar) y la autenticación de código (es decir, firmado por la autoridad competente).

Las claves privadas con firma de código se almacenan en un hardware seguro, (por ejemplo, IBM 4767 Cryptographic Coprocessor) tras un cortafuegos con el acceso restringido y controles de auditoría plenos.

Certificación remota de software del sistema

El módulo de plataforma fiable (TPM) permite la certificación remota de la pila de código en un sistema en ejecución. La cadena de firmware de confianza registra el hash del firmware que se carga y almacena los registros en la red de los TPM Arranque seguro. La red puede tener un TPM físico por procesador maestro en plataformas basadas en procesadores POWER9. La certificación da soporte al arranque de confianza compatible con Trusted Computing Group (TCG) 2.0. La infraestructura de TPM identificada soporta pilas de certificación futura.

Las interfaces de certificación física permiten que un cliente tercero de confianza recupere información sobre el estado de arranque de confianza del sistema PowerVM de destino. Este proceso utiliza los TPM físicos del sistema que son dispositivos compatibles con TCG 2.0. El firmware del sistema utiliza estos TPM para ampliar mediciones durante el proceso de arranque.

Avisos

Esta información se ha desarrollado para productos y servicios ofrecidos en EE.UU.

Es posible que IBM no ofrezca en otros países los productos, servicios o características descritos en este documento. Solicite información al representante local de IBM acerca de los productos y servicios disponibles actualmente en su zona. Cualquier referencia a un producto, programa o servicio de IBM no pretende afirmar ni implicar que sólo pueda utilizarse ese producto, programa o servicio de IBM. En su lugar, se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no infrinja los derechos de propiedad intelectual de IBM. No obstante, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patente pendientes de aprobación que cubran los temas descritos en este documento. La posesión de este documento no le confiere ninguna licencia sobre dichas patentes. Puede enviar consultas sobre licencias, por escrito, a:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
EE.UU.

Para realizar consultas sobre licencias relacionadas con la información del juego de caracteres de doble byte (DBCS), póngase en contacto con el departamento de propiedad intelectual de IBM en su país o envíe sus consultas, por escrito, a:

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

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍAS DE NINGUNA CLASE, YA SEAN EXPRESAS O IMPLÍCITAS, INCLUYENDO, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE NO INFRACCIÓN, COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN DETERMINADO. Algunas jurisdicciones no permiten la renuncia de garantías expresas o implícitas en ciertas transacciones, por lo que esta declaración podría no ser aplicable en su caso.

Esta información puede contener imprecisiones técnicas o errores tipográficos. La información incluida en este documento está sujeta a cambios periódicos, que se incorporarán en nuevas ediciones de la publicación. IBM puede efectuar mejoras y/o cambios en el producto(s) y/o el programa(s) descritos en esta publicación en cualquier momento y sin previo aviso.

Cualquier referencia hecha en esta información a sitios web que no sean de IBM se proporciona únicamente para su comodidad y no debe considerarse en modo alguno como promoción de dichos sitios web. Los materiales de estos sitios web no forman parte de los materiales de IBM para este producto y el uso que se haga de estos sitios web es de la entera responsabilidad del usuario.

IBM puede utilizar o distribuir la información que se le suministre de cualquier modo que considere adecuado sin incurrir por ello en ninguna obligación con el remitente.

Los titulares de licencias de este programa que deseen obtener información acerca de éste con el fin de permitir: (i) el intercambio de información entre programas creados independientemente y otros programas (incluido éste) y (ii) la utilización mutua de la información que se ha intercambiado, deben ponerse en contacto con:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
EE.UU.

Esta información podría estar disponible, de acuerdo con los términos y condiciones correspondientes, incluyendo en algunos casos el pago de una tarifa.

IBM proporciona el programa bajo licencia que se describe en este documento y todo el material bajo licencia disponible para el mismo bajo los términos del Acuerdo de cliente de IBM, el Acuerdo internacional de licencias de programas de IBM o cualquier acuerdo equivalente entre las partes.

Los ejemplos de datos de rendimiento y de clientes citados se presentan solamente a efectos ilustrativos. Los resultados reales de rendimiento pueden variar en función de configuraciones específicas y condiciones de operación.

La información concerniente a productos que no sean de IBM se ha obtenido de los suministradores de dichos productos, de sus anuncios publicados o de otras fuentes de información pública disponibles. IBM no ha probado estos productos y no puede confirmar la exactitud del rendimiento, la compatibilidad o cualquier otra afirmación relacionada con productos que no son de IBM. Las consultas acerca de las prestaciones de los productos que no sean de IBM deben dirigirse a las personas que los suministran.

Las declaraciones relacionadas con las futuras directrices o intenciones de IBM están sujetas a cambios o a su retirada sin previo aviso y sólo representan metas u objetivos.

Todos los precios IBM que se muestran son precios de venta al público sugeridos por IBM, son actuales y están sujetos a cambios sin previo aviso. Los precios de los distribuidores pueden variar.

Esta documentación se suministra sólo a efectos de planificación. La información que aquí se incluye está sujeta a cambios antes de que los productos descritos estén disponibles.

Esta información contiene ejemplos de datos e informes utilizados en operaciones comerciales diarias. Para ilustrarlas de la forma más completa posible, los ejemplos incluyen nombres de personas, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier similitud con nombres reales de personas o empresas es mera coincidencia.

LICENCIA DE COPYRIGHT:

Esta información contiene programas de aplicación de ejemplo en lenguaje fuente que ilustran las técnicas de programación en diversas plataformas operativas. Puede copiar, modificar y distribuir estos programas de ejemplo de cualquier forma y sin pagar a IBM, para las finalidades de desarrollar, utilizar, comercializar o distribuir programas de aplicación que se ajusten a la interfaz de programación de aplicaciones para la plataforma operativa para la que se han escrito los programas. Estos ejemplos no se han sometido a pruebas exhaustivas bajo todas las condiciones. Por lo tanto, IBM no puede garantizar ni implicar la fiabilidad, la capacidad de servicio ni el funcionamiento de estos programas. Los programas de ejemplo se proporcionan "TAL CUAL", sin garantías de ningún tipo. IBM no será responsable de los daños derivados de la utilización de los programas de ejemplo por parte del cliente.

Cada copia o cada parte de los programas de ejemplo o de los trabajos que se deriven de ellos debe incluir un aviso de copyright, tal como se indica a continuación:

© (nombre de su empresa) (año).
Partes de este código proceden de los
programas de ejemplo de IBM Corp.
© Copyright IBM Corp. _especifique el año o años_.

Si está viendo esta información en copia software, es posible que las fotografías y las ilustraciones en color no aparezcan.

Funciones de accesibilidad para servidores IBM Power Systems

Las funciones de accesibilidad ayudan a los usuarios con discapacidades como, por ejemplo, movilidad restringida o visión limitada, a la hora de utilizar el contenido de las tecnologías de la información de forma correcta.

Visión general

Los servidores IBM Power Systems incluyen estas funciones de accesibilidad principales:

- Funcionamiento solo con teclado
- Operaciones que utilizan un lector de pantalla

Los servidores IBM Power Systems utilizan el estándar W3C más reciente, WAI-ARIA 1.0 (www.w3.org/TR/wai-aria/), con el fin de garantizar la conformidad con la US Section 508 (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) y las directrices Web Content Accessibility Guidelines (WCAG) 2.0 (www.w3.org/TR/WCAG20/). Para aprovechar les funciones de accesibilidad, utilice la versión más reciente del su lector de pantalla y el navegador web más reciente que admitan los servidores IBM Power Systems.

La documentación en línea de productos de servidores IBM Power Systems de IBM Knowledge Center está habilitada para las funciones de accesibilidad. Las funciones de accesibilidad de IBM Knowledge Center se describen en la Sección de accesibilidad de la ayuda de IBM Knowledge Center (www.ibm.com/support/knowledgecenter/doc/kc_help.html#accessibility).

Navegación con teclado

Este producto utiliza las teclas de navegación estándar.

Información sobre la interfaz

Las interfaces de usuario de los servidores IBM Power Systems no disponen de contenido que parpadee entre 2 y 55 veces por segundo.

La interfaz de usuario de web de los servidores IBM Power Systems se basan en hojas de estilo en cascada para representar el contenido correctamente y para ofrecer una experiencia útil. La aplicación proporciona una forma equivalente para que los usuarios con visión reducida utilicen los valores de visualización del sistema, incluida la modalidad de alto contraste. Puede controlar la medida de la letra mediante los valores del dispositivo o del navegador web.

La interfaz de usuario de los servidores IBM Power Systems incluye puntos de referencia de navegación WAI-ARIA que se pueden utilizar para navegar de forma rápida a áreas funcionales de la aplicación.

Software de proveedores

Los servidores IBM Power Systems incluyen software de determinados proveedores que no está cubierto en el acuerdo de licencia de IBM. IBM no se hace responsable de las funciones de accesibilidad de estos

productos. Póngase en contacto con el proveedor si necesita información sobre la accesibilidad en estos productos.

Información relacionada con la accesibilidad

Además del centro de atención al cliente de IBM y de los sitios web de ayuda técnica, IBM dispone de un servicio telefónico de teletipo para que las personas sordas o con dificultades auditivas puedan acceder a los servicios de ventas y soporte técnico:

Servicio TTY
800-IBM-3383 (800-426-3383)
(en Norteamérica)

Para obtener más información sobre el compromiso de IBM en cuanto a la accesibilidad, consulte IBM Accessibility (www.ibm.com/able).

Consideraciones de la política de privacidad

Los productos de IBM Software, incluido el software como soluciones de servicio, (“Ofertas de software”) pueden utilizar cookies u otras tecnologías para recopilar información de uso del producto, para ayudar a mejorar la experiencia del usuario final, para adaptar las interacciones con el usuario final o para otros fines. En muchos casos, las ofertas de software no recopilan información de identificación personal. Algunas de nuestras ofertas de software pueden ayudarle a recopilar información de identificación personal. Si esta Oferta de software utiliza cookies para recopilar información de identificación personal, a continuación se describe información específica sobre la utilización de cookies por parte de esta oferta.

Esta Oferta de software no utiliza cookies u otras tecnologías para recopilar información de identificación personal.

Si las configuraciones desplegadas para esta oferta de software le ofrecen como cliente la posibilidad de recopilar información de identificación personal de los usuarios finales mediante cookies y otras tecnologías, debe buscar asesoramiento jurídico sobre la legislación aplicable a esa recopilación de datos, que incluye cualquier requisito de aviso y consentimiento.

Para obtener más información sobre el uso de las diversas tecnologías, incluidas las cookies, para estos fines, consulte la política de privacidad de IBM en http://www.ibm.com/privacy y la declaración de privacidad en línea de IBM en http://www.ibm.com/privacy/details la sección “Cookies, Web Beacons and Other Technologies” e “IBM Software Products and Software-as-a-Service Privacy Statement” en http://www.ibm.com/software/info/product-privacy.

Información de la interfaz de programación

Este arranque seguro en la publicación PowerVM documenta interfaces de programación concebidos para permitir al cliente escribir programas para obtener servicios de IBM AIX Versión 7.2, IBM AIX Versión 7.1, IBM AIX Versión 6.1, IBM i 7.3 y IBM Servidor de E/S virtual Versión 3.1.0.0.

Marcas registradas

IBM, el logotipo de IBM, e ibm.com son marcas registradas de International Business Machines Corp., registradas en muchas jurisdicciones en todo el mundo. Otros nombres de productos y servicios pueden ser marcas registradas de IBM o de otras empresas. Puede consultar una lista actualizada de las marcas registradas de IBM en la web, en la sección Copyright and trademark information en la dirección www.ibm.com/legal/copytrade.shtml.

Términos y condiciones

El permiso para utilizar estas publicaciones se otorga de acuerdo a los siguientes términos y condiciones.

Aplicabilidad: estos términos y condiciones son adicionales a los términos de uso del sitio web de IBM.

Uso personal: puede reproducir estas publicaciones para uso personal (no comercial) siempre y cuando incluya una copia de todos los avisos de derechos de autor. No puede distribuir ni visualizar estas publicaciones ni ninguna de sus partes, como tampoco elaborar trabajos que se deriven de ellas, sin el consentimiento explícito de IBM.

Uso comercial: puede reproducir, distribuir y visualizar estas publicaciones únicamente dentro de su empresa, siempre y cuando incluya una copia de todos los avisos de derechos de autor. No puede elaborar trabajos que se deriven de estas publicaciones, ni tampoco reproducir, distribuir ni visualizar estas publicaciones ni ninguna de sus partes fuera de su empresa, sin el consentimiento explícito de IBM.

Derechos: Excepto lo expresamente concedido en este permiso, no se conceden otros permisos, licencias ni derechos, explícitos o implícitos, sobre las publicaciones ni sobre ninguna información, datos, software u otra propiedad intelectual contenida en el mismo.

IBM se reserva el derecho de retirar los permisos aquí concedidos siempre que, según el parecer del fabricante, se utilicen las publicaciones en detrimento de sus intereses o cuando, también según el parecer de IBM, no se sigan debidamente las instrucciones anteriores.

No puede descargar, exportar ni reexportar esta información si no lo hace en plena conformidad con la legislación y normativa vigente, incluidas todas las leyes y normas de exportación de Estados Unidos.

IBM NO PROPORCIONA NINGUNA GARANTÍA SOBRE EL CONTENIDO DE ESTAS PUBLICACIONES. LAS PUBLICACIONES SE PROPORCIONAN "TAL CUAL", SIN GARANTÍA DE NINGUNA CLASE, YA SEA EXPLÍCITA O IMPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN, NO VULNERACIÓN E IDONEIDAD PARA UN FIN DETERMINADO.

Impreso en España