Actualización de información de PowerEdge T640: hoja técnica

Junio del 2022
Rev. 1

DELL Technologies

Notas, precauciones y avisos

NOTA: Una NOTA indica información importante que le ayuda a hacer un mejor uso de su producto.

PRECAUCIÓN: Una PRECAUCIÓN indica la posibilidad de daños en el hardware o la pérdida de datos, y le explica cómo evitar el problema.

AVISO: Un mensaje de AVISO indica el riesgo de daños materiales, lesiones corporales o incluso la muerte.

Tabla de contenido

1

Descripción general

La información de este documento reemplaza la información en las secciones pertinentes del Manual de instalación y servicio, la Guía de referencia de BIOS y UEFI, y las Especificaciones técnicas.

Para obtener la información completa, consulte los documentos disponibles en https://www.dell.com/poweredgemanuals.

2

Actualización de información

Temas:

Conectores del backplane

En función de la configuración, el sistema admite una de las configuraciones siguientes:

- Backplane SAS o SATA de 8 x 3,5 pulgadas
- Backplane SAS o SATA de 18 x 3,5 pulgadas
- Backplane Dell PowerEdge Express Flash (NVMe) de 8 x 2,5 pulgadas
- Backplane SAS o SATA de 16 x 2,5 pulgadas con los backplanes adicionales opcionales siguientes:
  - Backplane de unidad NVMe de 8 x 2,5 pulgadas
  - Backplane SAS o SATA de 16 x 2,5 pulgadas (FlexBay)
- Backplane SAS o SATA de 32 x 2,5 pulgadas

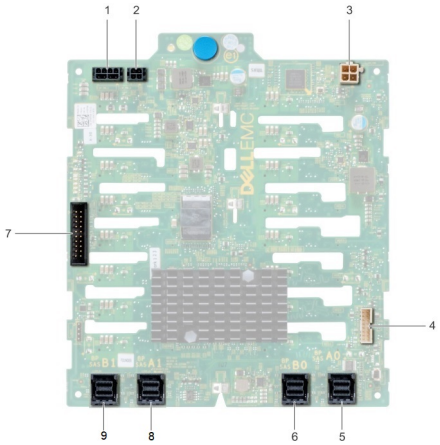

Ilustración 1. Backplane SAS o SATA de 16 x 2,5 pulgadas para FlexBay (superior)

1. conector de alimentación del backplane A [J_BP_PWR_A]
2. conector de alimentación del backplane B [J_BP_PWR_B]
3. conector de alimentación de las unidades ópticas [J_ODD_PWR]
4. conector de señal del backplane [J_BP_SIG]
5. Conector de SAS A0 [J_SAS_A0]
6. Conector de SAS B0 [J_SAS_B0]
7. Conector I2C
8. Conector de SAS A1 [J_EXP_A1]
9. Conector de SAS B1 [J_EXP_B1]

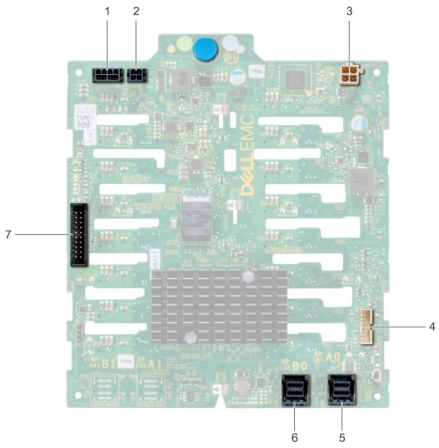

Ilustración 2. Backplane SAS o SATA de 16 x 2,5 pulgadas

1. conector de alimentación del backplane A [J_BP_PWR_A]
2. conector de alimentación del backplane B [J_BP_PWR_B]
3. conector de alimentación de las unidades ópticas [J_ODD_PWR]
4. conector de señal del backplane [J_BP_SIG]
5. Conector de SAS A0 [J_SAS_A0]
6. Conector de SAS B0 [J_SAS_B0]
7. Conector I2C

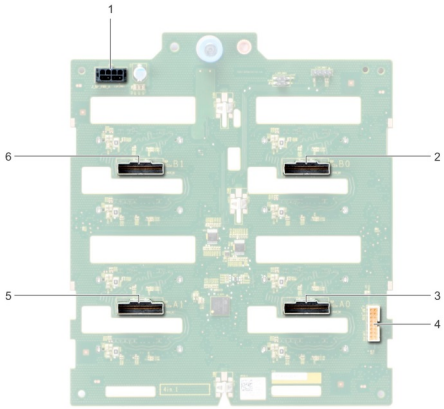

Ilustración 3. Backplane de unidad NVMe de 8 x 2,5 pulgadas

1. conector de alimentación del backplane [J_BP_PWR1]
2. Conector de PCIe B0 [J_PCIE_B0]
3. Conector de PCIe A0 [J_PCIE_A0]
4. conector de señal del backplane [J_BP_SIG1]
5. Conector de PCIe A1 [J_PCIE_A1]
6. Conector de PCIe B1 [J_PCIE_B1]

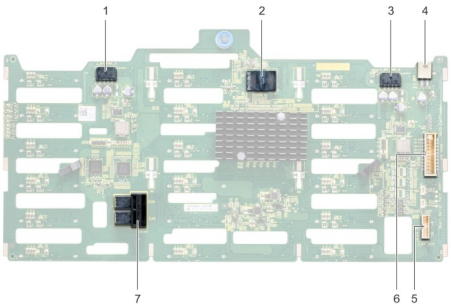

Ilustración 4. Backplane SAS o SATA de 18 x 3,5 pulgadas

1. conector de alimentación del backplane A [J_BP_PWR_A1]
2. controladora
3. conector de alimentación del backplane B [J_BP_PWR_B1]
4. conector de alimentación de las unidades ópticas [J_ODD1]
5. Conector I2C
6. conector de señal del backplane [J_BP_SIG1]
7. Conector de SAS A0_B0 [J_SAS_A0_B0]

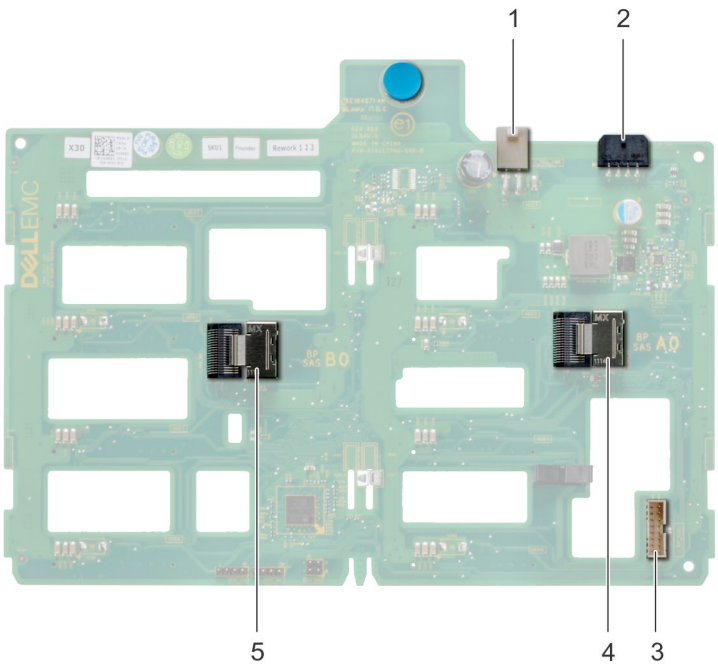

Ilustración 5. Backplane SAS o SATA de 8 x 3,5 pulgadas

1. conector de alimentación de las unidades ópticas [J_ODD1]
2. conector de alimentación del backplane [J_BP_PWR_A]
3. conector SAS A0 [J_BP_SIG]
4. conector de señal del backplane [J_SAS_A0]
5. Conector de SAS B0 [J_SAS_B0]

Seguridad del sistema

Puede utilizar la pantalla **Seguridad del sistema** para realizar funciones específicas, por ejemplo, la configuración de la contraseña del sistema, la contraseña de configuración y deshabilitar el botón de encendido.

Visualización de la seguridad del sistema

Para ver la pantalla **System Security (Seguridad del sistema)**, realice los pasos a continuación:

Pasos

1. Encienda o reinicie el sistema.
2. Presione F2 inmediatamente después de ver el siguiente mensaje:

```
F2 = System Setup
```

NOTA: Si el sistema operativo comienza a cargar antes de presionar F2, espere a que el sistema termine de iniciar, reinícielo sistemae intente nuevamente.

3. En la pantalla **System Setup Main Menu (Menú principal de la configuración del sistema)**, haga clic en **System BIOS (BIOS del sistema)**.
4. En la pantalla **System BIOS (BIOS del sistema)**, haga clic en **System Security (Seguridad del sistema)**.

Detalles de configuración de seguridad del sistema

Sobre esta tarea

Los detalles de la pantalla **Configuración de seguridad del sistema** se indican a continuación:

Opción	Descripción
CPU AES-NI	Mejora la velocidad de las aplicaciones mediante el cifrado y descifrado con Advanced Encryption Standard Instruction Set (Conjunto de instrucciones de estándar de cifrado avanzado) y está establecida en Habilitado de manera predeterminada. Esta opción está establecida en **Habilitada** de manera predeterminada.
Contraseña del sistema	Permite establecer la contraseña del sistema. Esta opción está establecida en **Habilitada** de manera predeterminada y es de solo lectura si el puente de contraseña no está instalado en el sistema.
Contraseña de configuración	Permite establecer la contraseña de configuración del sistema. Esta opción es de solo lectura si el puente de contraseña no está instalado en el sistema.
Estado de contraseña	Permite bloquear la contraseña del sistema. De manera predeterminada, esta opción está establecida en **Desbloqueado**.
Seguridad del TPM	**NOTA:** El menú TPM solo está disponible cuando el módulo TPM está instalado. Le permite controlar el modo de información del módulo de plataforma de confianza (TPM). De manera predeterminada, la opción **Seguridad del TPM** está establecida en **Desactivado**. Solo puede modificar los campos estado del TPM, activación del TPM e Intel TXT si el campo **Estado del TPM** está establecido en **Encendido con medidas previas al arranque** o **Encendido sin medidas previas al arranque**.
Información de TPM	Permite cambiar el estado de funcionamiento del TPM. Esta opción está establecida en **Tipo: 2.0-NTZ** de forma predeterminada.
Estado de TPM	Especifica el estado del TPM.
Comando TPM	Controla el Módulo de plataforma de confianza (TPM). Cuando se establece en **Ninguno**, no se envía ningún comando en el TPM. Si se establece en **Activado**, el TPM se habilitará y se activará. Si se establece en **Desactivado**, el TPM se deshabilitará y se desactivará. Cuando esta opción se establece en **Borrar**, se borra todo el contenido del TPM. De manera predeterminada, esta opción está establecida en **Ninguno**. **PRECAUCIÓN: Si se borran los resultados del TPM, se perderán todas las claves del TPM, lo que podría afectar el inicio del sistema operativo.** Este campo es de solo lectura cuando la opción **Seguridad del TPM** se establece en **Desactivada**. La acción requiere un reinicio adicional para surtir efecto.
Jerarquía de TPM	Permite la activación, la desactivación o el borrado de las jerarquías de almacenamiento y aprobación. Si se configura en **Habilitado**, las jerarquías de aprobación y almacenamiento se pueden usar. Si se configura en **Deshabilitado**, las jerarquías de aprobación y almacenamiento no se pueden usar. Si se configura en **Borrar**, se borra cualquier valor de las jerarquías de aprobación y almacenamiento y, luego, se restablece la opción en **Habilitado**.
Configuración avanzada de TPM	Esta configuración solo está habilitada cuando la seguridad del TPM está establecida en encendida.
Intel(R) TXT	Permite establecer la opción Trusted Execution Technology (TXT) de Intel. Para activar la opción **TXT de Intel**, las opciones Tecnología de virtualización y Seguridad del TPM deben estar establecida en Habilitado con mediciones previas al inicio. De manera predeterminada, esta opción está establecida en **Desactivada**.
Botón de encendido	Permite establecer el botón de encendido en la parte frontal del sistema. Esta opción está establecida en **Habilitada** de manera predeterminada.
Recuperación de alimentación de CA	Permite establecer la reacción del sistema después de que se restablezca la alimentación de CA del sistema. De manera predeterminada, esta opción está establecida en **Última**.
Demora de recuperación de alimentación de CA	Permite establecer el tiempo que el sistema debería demorar en encender después de que se restaura la alimentación de CA al sistema. De manera predeterminada, esta opción está establecida en **Inmediato**.
Demora definida por el usuario (60 s a 600 s)	Permite establecer la opción **Demora definida por el usuario** cuando se selecciona la opción **Definida por el usuario** para **Demora de recuperación de alimentación de CA**.
Acceso de variable de UEFI	Proporciona diversos grados de variables UEFI de garantía. Cuando está establecida en **Estándar** (valor predeterminado), las variables UEFI son accesibles en el sistema operativo por la especificación UEFI. Cuando se establece en **Controlada**, las variables de UEFI seleccionadas están protegidas en el ambiente y se fuerzan las nuevas entradas de arranque de UEFI al final del orden de arranque actual.

Opción	Descripción
Interfaz de facilidad de administración dentro de banda	Si se establece en **Desactivado**, este valor ocultará los dispositivos HECI del motor de administración (ME) y los dispositivos IPMI del sistema operativo. Esto evita que el sistema operativo a la de cambiar el límite de alimentación ME configuración, y bloquea el acceso a todos los dentro de banda las herramientas de administración. Toda la administración debe ser administrada a través de fuera de banda. Esta opción está establecida en **Habilitada** de manera predeterminada. **NOTA:** Actualización del BIOS precisa HECI dispositivos estar en funcionamiento y DUP actualizaciones requieren interfaz IPMI sea operativo. Este valor se debe establecer en **Habilitada** para evitar errores de actualización.
Arranque seguro	Habilita el arranque seguro, donde el BIOS autentica cada imagen de inicio previo usando los certificados de la política de inicio seguro. De manera predeterminada, el arranque seguro está establecido en **Deshabilitado**.
Política de arranque seguro	Cuando la política de arranque seguro se establece en **Estándar**, el BIOS usa los certificados y la clave del fabricante del sistema para autenticar las imágenes previas al arranque. Cuando la política de inicio seguro está establecida en **Personalizada**, el BIOS utiliza las claves y los certificados definidos por el usuario. La política de inicio seguro está establecida en **Estándar** de manera predeterminada.
Modo de arranque seguro	Permite configurar cómo el BIOS usa los objetos de política de arranque seguro (PK, KEK, db, dbx). Si el modo actual se establece en **Modo implementado**, las opciones disponibles son **Modo de usuario** y **Modo implementado**. Si el modo actual se establece en **Modo de usuario**, las opciones disponibles son **Modo de usuario**, **Modo de auditoría** y **Modo implementado**.

Opciones	Descripción
Modo de usuario	En **Modo de usuario**, PK debe estar instalada y verificación de la firma DEL BIOS realiza en programación intenta actualizar los objetos de directiva. El BIOS permite transiciones programáticas no autenticadas entre los modos.
Modo de auditoría	En **Modo de auditoría**, PK no está presente. El BIOS no autentica actualizaciones programáticas a los objetos de política y realiza transiciones entre modos. El **Modo de auditoría** es útil para determinar, mediante programación, un espacio de trabajo de objetos El BIOS realiza la verificación de la firma en las imágenes previas al arranque. El BIOS también registra los resultados en la tabla de información de ejecución de imagen, pero aprueba las imágenes pasen o no la verificación.
Modo implementado	El **Modo implementado** es el modo más seguro. En **Modo implementado**, PK debe estar instalado y el BIOS realiza verificación de la firma en programación intenta actualizar los objetos de directiva. El **Modo implementado** restringe las transiciones de modo programático.

Resumen de política de arranque seguro	Muestra la lista de certificados y hashes que el inicio seguro utiliza para autenticar las imágenes.
Configuración de la política personalizada de arranque seguro	Configura la política personalizada de arranque seguro. Para habilitar esta opción, establezca la **Política de arranque seguro** a **Personalizado**.