Refuerce la seguridad con

3,5 veces más características de seguridad

Incluye autenticación de dos factores y gestión de claves externas con iDRAC9

Optimice la eficiencia energética con más de

6 veces más de informes de consumo de energía

Con 20 informes en Dell OME frente a 3 informes en Supermicro SSM

Aumente la eficiencia operativa ahorrando 1 h y 50 minutos en tiempo de administración

por cada 100 servidores

Uso de actualizaciones automáticas con Dell iDRAC9 en lugar de actualizaciones automáticas no disponibles con Supermicro IPMI

Aumente la seguridad, la sostenibilidad y la eficiencia con las sólidas herramientas de gestión de servidores de Dell

En comparación con la cartera de gestión de Supermicro

Cuando invierte en nuevos servidores para su centro de datos, está haciendo algo más que solo seleccionar hardware; también está eligiendo una solución de capacidad de gestión. Cuando los administradores disponen de herramientas eficientes y repletas funciones para implementar, supervisar, mantener y proteger su infraestructura a la vez que mejoran su eficiencia energética, pueden encargarse fácilmente de la gestión diaria y dedicar más tiempo a innovaciones que hagan avanzar a su organización. Al elegir comprar a un proveedor con herramientas de capacidad de gestión sólidas, podría ahorrarse tiempo y dinero en el futuro.

Hemos evaluado las carteras de gestión de servidores de Dell™ y Supermicro®, comparando tres herramientas de Dell con dos de Supermicro.

Tabla 1: Las herramientas de gestión que hemos probado. *Dell CloudIQ es una herramienta de supervisión y análisis basada en la cloud; Supermicro no ofrece ninguna herramienta equivalente.
Fuente: Principled Technologies.

	Dell	Supermicro
Gestión de servidores integrada/remota	iDRAC9 (Integrated Dell Remote Access Controller)	Supermicro Intelligent Management (IPMI)
Consola de gestión de dispositivos de uno a varios	Dell OpenManage™ Enterprise (OME) Dell CloudIQ*	Supermicro Server Manager (SSM)

En cuanto a la sostenibilidad, la seguridad y la experiencia de gestión diaria, descubrimos que Dell proporcionaba de forma constante conjuntos de herramientas más completos de funciones que dotan a los administradores de más opciones y capacidades.

Más funciones, y más completas, para automatizar y facilitar la gestión de servidores

Sus equipos de TI necesitan herramientas de gestión modernas y repletas de funciones que les permitan ahorrar tiempo en su trabajo diario y mantenerse al día con los estándares de seguridad y eficiencia. Las herramientas de gestión de Dell que evaluamos incluyen una serie de características y capacidades que no están presentes en la cartera de gestión de Supermicro.

Sostenibilidad

A medida que aumentan los costes de la energía y las normativas medioambientales, muchas organizaciones están centrando su atención en la sostenibilidad. Los centros de datos requieren de forma inherente grandes cantidades de energía, pero una gestión cuidadosa del consumo térmico y de energía puede permitir a las organizaciones reducir la cantidad de energía que consumen. Dell OpenManage Enterprise incorpora varias funciones que pueden permitir una supervisión y gestión minuciosas del consumo de energía, lo que podría ayudarle a alcanzar sus objetivos de sostenibilidad. En las tablas 2 y 3 se destacan las ventajas clave de estas funciones, que describimos con mayor detalle a continuación.

Tabla 2: Diferencias en sostenibilidad entre Dell OpenManage Enterprise y SSM. Fuente: Principled Technologies.

Característica	Herramientas de gestión de Dell	Herramientas de gestión de Supermicro
Calculadora de uso de emisiones de carbono y herramienta de planificación de la capacidad	✓	x
Análisis de la huella de carbono	✓	x
Política de administración de energía activada por la temperatura	✓	x
Política de administración de energía estática	✓	✓

Tabla 3: Resumen de nuestra comparación entre Dell OME y Supermicro SSM e IPMI. Fuente: Principled Technologies.

Característica	Ventajas clave de las herramientas de gestión de Dell	Desventaja con las herramientas de gestión de Supermicro
Calculadora de uso de emisiones de carbono y herramienta de planificación de la capacidad	Capacidad para estimar las **emisiones de gases de efecto invernadero** con valores personalizables que le ayudarán a cumplir sus objetivos de sostenibilidad	**No hay función comparable**; dificulta la planificación para ayudarle a cumplir sus objetivos de sostenibilidad
Análisis de la huella de carbono	**Disponible** a través de OpenManage Enterprise Power Manager; proporciona datos sobre las emisiones de carbono, que pueden ayudarle a cumplir los objetivos de sostenibilidad	**No hay función comparable**; sin forma de realizar un seguimiento de la huella de carbono para ayudarle a supervisar el cumplimiento de sus objetivos de sostenibilidad
Gestión automatizada de la energía y la temperatura	Opciones de **políticas estáticas y activadas por temperatura** con la opción de activarse cuando el servidor supera un umbral de consumo de energía o temperatura	**Un tipo de política estática** sin opciones de activación asociadas
Informes de consumo de energía	**Más de 6 veces** más informes, con **20** informes integrados con opciones de personalización y distribución por correo electrónico programadas	**2 informes integrados** en SSM; 1 informe en Supermicro IPMI que no es exportable
Métricas de administración de energía	Hasta **15 veces más métricas**, lo que ofrece información más detallada sobre la administración del consumo de energía	**Solo 1**, lo que proporciona menos información y control del consumo de energía

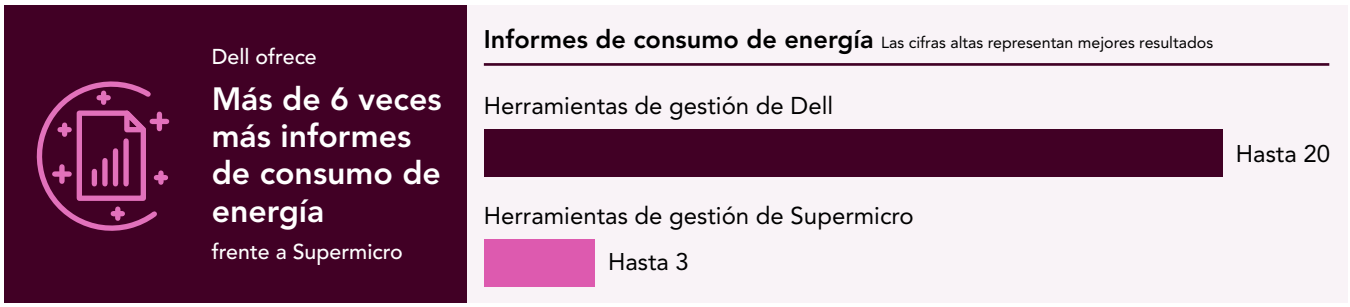

Figura 1: Número de informes de consumo de energía disponibles en Dell OME y Supermicro SSM. Fuente: Principled Technologies.

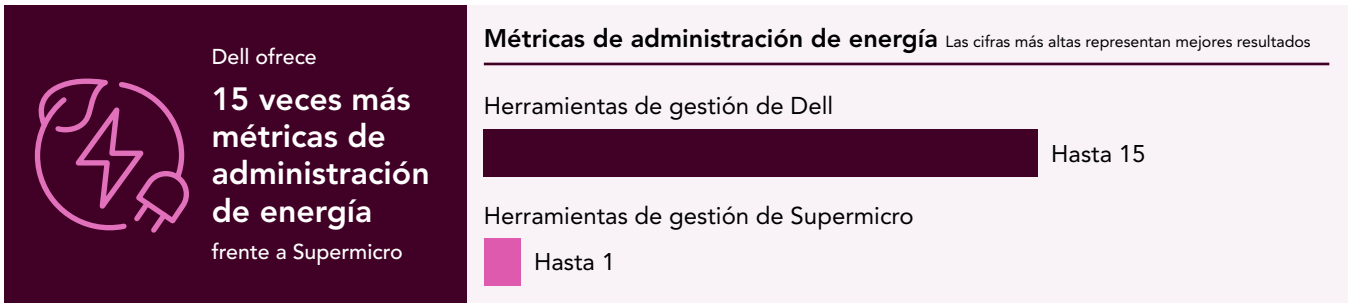

Figura 2: Número de métricas de administración de energía disponibles en Dell OME y Supermicro SSM. Fuente: Principled Technologies.

Gestión automatizada de la energía y la temperatura

OpenManage Enterprise Power Manager ofrece administración automatizada de la energía y la temperatura a través de opciones de políticas activadas por la energía estática y la temperatura que permiten a los administradores establecer límites para el consumo de energía o umbrales de temperatura para ayudar a reducir los costes de refrigeración. Por el contrario, SSM tiene una única política, un límite estático en el consumo de energía que no se activa automáticamente cuando un servidor supera el límite, lo que podría llevar a mayores costes de energía.

Las organizaciones que buscan una inmersión profunda en el consumo de energía de su centro de datos con un enfoque en la optimización pueden beneficiarse de los **20 informes de consumo de energía integrados diferentes** que OpenManage Enterprise Power Manager ofrece. Estos informes son útiles en la planificación de la capacidad y la administración de la energía para maximizar la eficiencia. Las opciones de creación de informes en SSM son mucho más limitadas. Los administradores solo pueden ejecutar un solo host con un informe de servicio o ver una tendencia de consumo de energía en la pantalla de supervisión. Con Supermicro IPMI, los usuarios pueden ver un gráfico de energía de nivel de componente en la BMC; sin embargo, no pueden exportar los datos del gráfico para su análisis y solo pueden guardarlos como una imagen.

El plugin OpenManage Enterprise Power Manager permite a los administradores **ver hasta 15 métricas diferentes**, lo que incluye el uso de energía por componentes individuales, el flujo de aire y el uso de componentes, mientras que SSM solo ofrece el uso total de energía.

Análisis de emisiones de carbono y huella de carbono

OME incluye una calculadora de uso de emisiones de carbono y una herramienta de planificación de la capacidad que, entre otras funciones, pueden ayudarle a calcular sus propias emisiones de gases de efecto invernadero. Proporciona valores predeterminados para los costes de energía y las emisiones de carbono de una unidad de energía consumida, pero le permite personalizar esos valores para los costes de energía de su región y el modelo de consumo de su centro de datos. SSM no ofrece ninguna función comparable, lo que puede dificultar a las organizaciones planificar y supervisar el progreso hacia sus objetivos de sostenibilidad.

Seguridad

La ciberdelincuencia está aumentando exponencialmente, amenazando a las empresas con "daños y destrucción de datos, dinero robado, pérdida de productividad, robo de propiedad intelectual, robo de datos personales y financieros, malversación, fraude, interrupción después del ataque en el curso normal de los negocios, investigación forense, restauración y eliminación de datos y sistemas pirateados, y daño a la reputación".[1] En este panorama, los responsables de la toma de decisiones deben tener en cuenta la seguridad en cualquier compra de servidores. Hemos determinado que Dell OpenManage Enterprise incorpora varias funciones para ayudar a mantener sus datos protegidos que las herramientas de Supermicro no tienen (consulte las tablas 4 y 5).

Tabla 4: Diferencias de seguridad entre las herramientas de gestión de Dell y las herramientas de gestión de Supermicro.
Fuente: Principled Technologies.

Característica	Herramientas de gestión de Dell	Herramientas de gestión de Supermicro
Autenticación multifactor	✓	x
Gestión de claves externas	✓	x
Controles de acceso basado en el alcance	✓	x
Acceso seguro basado en políticas	✓	x
Asesorías sobre ciberseguridad	✓	x
Controles de acceso basado en funciones	✓	✓
Desactivación dinámica de puertos USB	✓	✓

Tabla 5: Resumen de nuestra comparación de características de seguridad entre las herramientas de gestión de Dell y Supermicro.
Fuente: Principled Technologies.

Característica	Ventajas clave de las herramientas de gestión de Dell	Desventaja con las herramientas de gestión de Supermicro
Autenticación multifactor (MFA)	**Autenticación de dos factores** con iDRAC con **correo electrónico y RSA SecurID**, lo que evita que los usuarios no autorizados obtengan acceso a datos confidenciales	**No hay función comparable**, lo que deja una brecha de seguridad que podría ayudar a los usuarios no autorizados a acceder a datos confidenciales
Gestión de claves externas	**Secure Enterprise Key Manager** en iDRAC para añadir otra capa de seguridad para proteger los datos en reposo en los servidores mediante el cifrado de unidades y la gestión centralizada	**No hay función comparable**, lo que deja otra brecha en la seguridad
Controles de acceso	OME ofrece **tanto** control de acceso basado en funciones **(RBAC)** como control de acceso basado en el alcance **(SBAC)** para limitar los grupos de dispositivos a los que tiene acceso un administrador de dispositivos	**Solo RBAC**, lo que limita la capacidad de los administradores para restringir el acceso
Acceso seguro basado en políticas	**Configuración de seguridad basada en políticas** a través de CloudIQ, que alerta a los administradores de las discrepancias	**No hay función comparable**, lo que puede retrasar la acción y la corrección de vulneraciones
Asesorías sobre ciberseguridad	**Informes de asesoría de seguridad** a través de la seguridad de Dell CloudIQ, con detalles de vulnerabilidad y sugerencias de corrección aplicables para permitir una acción rápida	**No hay función comparable**, lo que deja brechas de seguridad para que los actores malintencionados las exploten

Autenticación multifactor

La autenticación multifactor (MFA) puede ayudar a evitar que usuarios no autorizados y actores malintencionados obtengan acceso a datos confidenciales. Hemos verificado que Dell iDRAC permite la autenticación de dos factores tanto con correo electrónico como con RSA SecurID, un conjunto de tecnologías de autenticación multifactor externas que se utilizan en muchos sectores.[2] También hemos verificado que ni Supermicro IPMI ni SSM ofrecen esta función, lo que deja una brecha de seguridad.

Gestión de claves

Los sistemas de gestión de claves externas (KMS) permiten a los equipos de TI utilizar un servidor independiente de terceros para gestionar las claves que utilizan para bloquear y desbloquear el almacenamiento de un servidor, lo que añade una capa de seguridad. iDRAC incluye Local Key Manager (LKM) para todos los nuevos servidores Dell PowerEdge. Algunas licencias también ofrecen Secure Enterprise Key Manager (SEKM), lo que permite una seguridad adicional con cifrado de disco completo y gestión de claves externas. SEKM es compatible con el protocolo OASIS KMIP estándar del sector, lo que permite a las organizaciones elegir cualquier proveedor externo de KMS que utilice ese estándar. Supermicro no ofrece esta función de seguridad ni una equivalente.

Controles de acceso

El control de acceso basado en funciones RBAC, donde la función de un usuario determina las partes del sistema a las que tiene acceso y las tareas que puede realizar allí, es un componente integral de muchas estrategias de seguridad de servidores. En OpenManage Enterprise, RBAC define los privilegios de usuario para tres funciones integradas: administrador, administrador de dispositivos y visualizador.[3] También ofrece control de acceso basado en el alcance (SBAC), que permite a los administradores limitar los grupos de dispositivos a los que tiene acceso un administrador de dispositivos.[4] Esto permite a los administradores proporcionar acceso a un subconjunto de dispositivos. Supermicro ofrece RBAC, pero no SBAC.

Gestión de credenciales

La rotación de contraseñas de iDRAC tiene varios propósitos: rota el acceso a OpenManage Enterprise de acuerdo con la política de seguridad, con un valor predeterminado mensual; funciona con un controlador de contraseñas externo y admite CyberArk para gestionar las contraseñas.[5,6]

Con OpenManage Enterprise, los administradores pueden gestionar la rotación de contraseñas de iDRAC reemplazando la necesidad de una cuenta de administrador estática conocida por una cuenta de servicio gestionada por OME. SSM no tiene esta capacidad.

Acceso seguro basado en políticas

Dell ofrece una función de ciberseguridad basada en políticas en la solución CloudIQ para PowerEdge AIOps. Esta función toma la configuración de un servidor PowerEdge implementado y lo compara con una política de configuración relacionada con la seguridad basada en los procedimientos recomendados de Dell. En caso de que CloudIQ detecte una discrepancia, notifica al administrador y proporciona los pasos para la corrección.[7] SSM no ofrece ninguna función equivalente, lo que podría suponer retrasos en la detección de vulneraciones.

Asesorías sobre ciberseguridad

Las asesorías sobre seguridad notifican al público sobre problemas de seguridad. Según Dell, la página de asesorías de seguridad de Dell en CloudIQ proporciona una lista completa de las asesorías de seguridad aplicables, junto con su impacto, el número de sistemas al que afectan y la fecha de publicación.[8] Dell CloudIQ proporciona informes de asesoría de seguridad con detalles de vulnerabilidades y sugerencias de corrección. SSM no ofrece una función similar, lo que podría dejar los sistemas vulnerables.

Acerca de Dell CloudIQ

Dell CloudIQ es una herramienta de AIOps basada en la cloud que ofrece "supervisión proactiva, aprendizaje automático y análisis predictivo" para una gran cantidad de productos y servicios de Dell, incluidos servidores, almacenamiento, dispositivos de protección de datos e infraestructura hiperconvergente.[9] En un estudio de Principled Technologies de 2022, descubrimos que CloudIQ tenía un impacto insignificante en el ancho de banda de la red, al tiempo que nos permitía supervisar la telemetría, el estado, las alertas y el inventario desde una sola consola.[10]

Obtenga más información sobre CloudIQ en https://www.dell.com/en-us/dt/solutions/cloudiq.htm.

Desactivación dinámica de puertos USB

La desactivación y activación de los puertos USB permite a los administradores controlar el acceso al servidor a través de un puerto USB, evitando así el uso malicioso y la introducción del riesgo de instalación de aplicaciones o virus prohibidos.

Dell iDRAC ofrece una desactivación independiente y dinámica de los puertos USB sin necesidad de tiempo de inactividad. Si bien Supermicro ofrece una desactivación dinámica de USB frontal (y USB posterior) dentro del BIOS, requiere la clave de licencia de Supermicro Datacenter Management Suite por nodo para habilitarla. El equipo de TI puede activarla implementando el comando de bloqueo del sistema, que se puede ejecutar desde BMC o la consola de Supermicro IPMI, pero no es independiente del modo de bloqueo del sistema.[11]

Como se muestra en la figura 3, deshabilitar los puertos con Dell iDRAC fue un proceso sencillo **que solo requirió 41 segundos y 4 pasos**, mientras que Supermicro IPMI tomó **más de cuatro veces más de duración, 2 minutos y 50 segundos y 6 pasos**. Extrapolando este ahorro de tiempo a 100 sistemas, el ahorro de tiempo aumentaría a 3 horas y 35 minutos, lo que significa que un administrador pasaría casi la mitad de una jornada laboral utilizando Supermicro IPMI en comparación con algo más de una hora con Dell iDRAC.

Figura 3: Tiempo para deshabilitar los puertos USB frontales para un solo servidor y tiempo extrapolado para deshabilitar los puertos USB frontales para 100 servidores.
Cuanto más bajo es mejor. Fuente: Principled Technologies.

Acerca de Dell OpenManage Enterprise

OpenManage Enterprise es una consola de administración de sistemas de tipo uno a muchos para el centro de datos. La consola ofrece una interfaz gráfica de usuario HTML5 moderna y se implementa como un dispositivo virtual para entornos VMware ESXi™, Microsoft Hyper-V y máquinas virtuales basadas en kernel (KVM). OpenManage Enterprise puede detectar e inventariar redes IPV4 e IPV6 para hasta 8000 dispositivos, incluidos servidores de montaje en rack Dell, servidores torre Dell, y blades y chasis Dell.[12] En un estudio reciente de PT, descubrimos que un entorno de Dell con OpenManage Enterprise y OpenManage Enterprise Modular (OME-M) puede ahorrar tiempo al realizar cambios en las VLAN y ayudar a evitar intervenciones durante las actualizaciones de firmware programadas.[13]

Obtenga más información acerca de OpenManage Enterprise en
https://www.dell.com/en-us/lp/dt/open-manage-enterprise

Supervisión, análisis y facilidad de uso

Las herramientas de capacidad de gestión varían enormemente en cuanto a la forma en que prestan asistencia a los administradores que llevan a cabo actividades de supervisión y análisis, así como otras tareas rutinarias, como programar actualizaciones. En esta sección, analizamos las diferencias en estas áreas entre las herramientas de gestión de Dell y Supermicro que estudiamos. Como descubrimos cuando investigamos las características de sostenibilidad y seguridad, la suite de herramientas de gestión de Dell ofrece numerosas funciones para facilitar la vida de los administradores, características que las herramientas de Supermicro no tienen. En la tabla 6 se comparan los beneficios de gestión que ofrecen las herramientas.

Tabla 6: Resumen de nuestra comparación entre las herramientas de gestión de Dell y Supermicro. Fuente: Principled Technologies.

Característica	Ventajas clave de las herramientas de gestión de Dell	Desventaja con las herramientas de gestión de Supermicro
Streaming de telemetría	**Streaming de telemetría** de iDRAC9 **disponible** para servidores Syslog remotos; ayuda a predecir fallos y optimizar el rendimiento; puede transmitir métricas de servidor a herramientas de análisis como Grafana y Splunk	**Sin streaming automático de telemetría**
Supervisión y gestión móvil	Aplicación OpenManage Mobile con muchas funciones para iOS y Android, que se integra con OME e iDRAC9	Aplicación Supermicro IPMIView, que **no se integra** con SSM
Supervisión de dispositivos y servidores de terceros	OME **admite la supervisión de dispositivos** y **servidores de terceros**, incluida la asistencia para sus principales competidores	**Solo admite dispositivos de terceros que utilicen sus agentes**, sus BMC, versiones anteriores de sus equipos compatibles con IPMI y dispositivos compatibles con Redfish
Supervisión de propiedad	Disponible a través de OME y CloudIQ; OME puede transmitir datos en servidores gestionados con licencia a CloudIQ para su supervisión en varios centros de datos	**No hay portal basado en la cloud** para agregar datos de supervisión en centros de datos
Acciones basadas en alertas	Políticas en OME que activan acciones basadas en la entrada de una alerta	**No hay acciones basadas en alertas disponibles**
Implementación de servidores más sencilla (capacidad para importar/exportar configuraciones del sistema)	Puede utilizar iDRAC9 para **importar/exportar** todos los elementos de configuración de los servidores, lo que requiere solo **48 segundos y 5 pasos para la importación y 1 minuto y 9 segundos y 7 pasos para la exportación**	Se puede importar/exportar **solo la configuración del controlador de gestión de la placa base (BMC)**, lo que requiere una configuración manual significativa para cada servidor
Menos tiempo para cambiar la configuración del BIOS	Puede cambiar rápidamente **la configuración completa del BIOS directamente desde iDRAC** y realizar la actualización y el reinicio para un intervalo de mantenimiento, lo que ahorra mucho tiempo de administración	**Cambios limitados en el BIOS disponibles** desde BMC; de lo contrario, es necesario reiniciar el servidor; requiere más pasos manuales y tiempo de administración
Se ejecuta como un dispositivo virtual	**Disponible** en OME, lo que elimina la necesidad de actualizar el sistema operativo	**No hay función comparable**, debe ejecutarse dentro de un SO gestionado. Esto proporciona a los administradores un componente más para aplicar parches y actualizar
Vista de conexión	**Disponible** en iDRAC; herramienta de solución de problemas con LLDP para diagnosticar problemas de red, como cableado, puertos de switch defectuosos y mucho más	**Sin vista de conexión**, no hay información de conectividad física sobre los puertos de switch ascendentes
Posibilidad de programar actualizaciones de firmware y controladores	**Disponible** en OME e iDRAC	Puede programar actualizaciones de firmware del BIOS y BMC, pero **no puede programar actualizaciones de controladores**

Cambio de elementos de configuración del BIOS

Dell ofrece cambios completos en la configuración del BIOS directamente desde iDRAC con la capacidad de realizar esos cambios para el siguiente reinicio. Supermicro ofrece un conjunto limitado de ajustes del BIOS desde su BMC. Aparte del conjunto limitado, un cambio en la configuración del BIOS en los servidores de Supermicro para un único elemento de configuración requiere que el administrador reinicie el servidor para acceder al menú de configuración del BIOS desde la pantalla de arranque.

En la figura 4 se muestra el tiempo necesario para realizar un cambio en la configuración del BIOS en un solo servidor con Dell iDRAC y Supermicro IPMI. El proceso manual con la **herramienta de Supermicro tarda 2 minutos y 6 segundos** o **más o 4,9 veces más** que configurar el proceso automatizado en iDRAC.
Si extrapolamos estos tiempos a 100 servidores que están configurados de forma idéntica, el ahorro de tiempo con iDRAC sería de 3,5 horas. (Si los servidores no estuvieran configurados de forma idéntica, no veríamos este ahorro de tiempo).

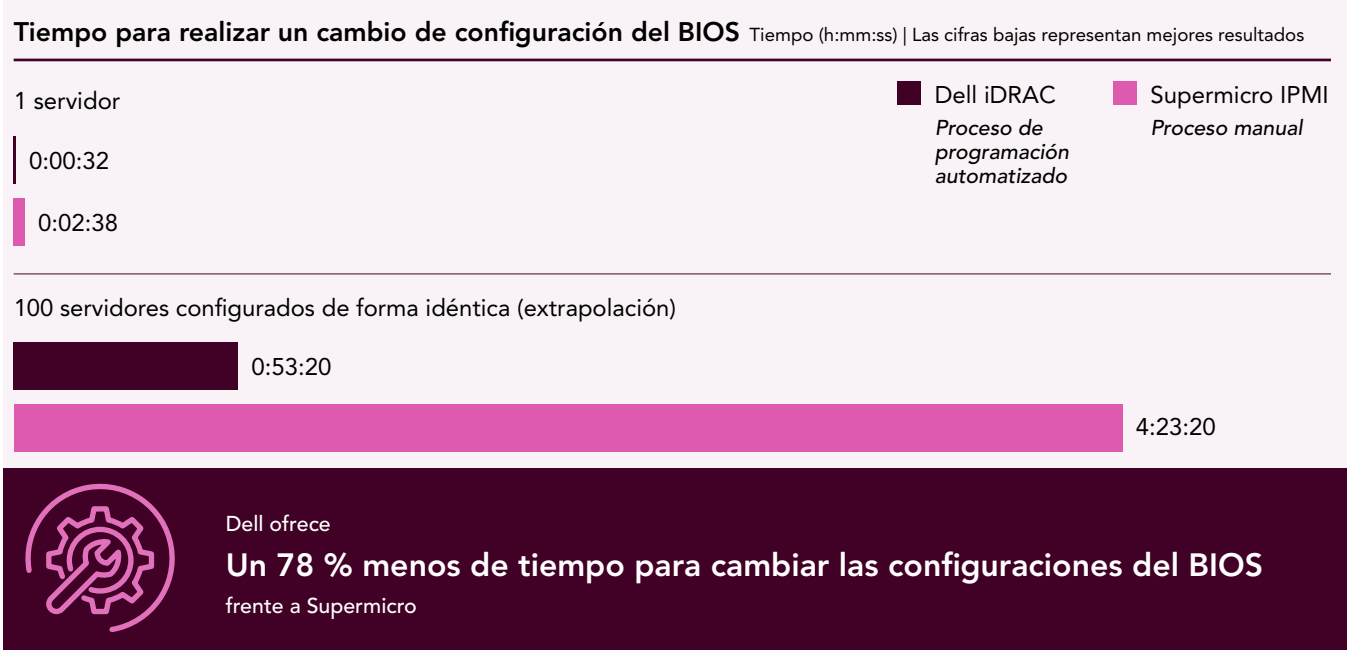

Figura 4: Tiempo para realizar un cambio en la configuración del BIOS tanto en un solo servidor como en 100 servidores configurados de forma idéntica (extrapolación).
Cuanto más bajo es mejor. Fuente: Principled Technologies.

Acerca de iDRAC9

Los servidores Dell PowerEdge™ incluyen Integrated Dell Remote Access Controller 9 con Dell Lifecycle Controller para proporcionar funciones de administración de sistemas que incluyen alertas del sistema y capacidades de gestión remota. Según Dell, las ventajas clave de iDRAC9 son:

- Capacidad de gestionar miles de servidores mediante API y herramientas de secuencias de comandos
- Compatibilidad integrada, que ofrece una vista del estado del servidor y la supervisión del estado de miles de parámetros
- Funciones y opciones de seguridad sólidas[14]

Para obtener más información sobre las funciones que ofrece iDRAC9, visite https://www.dell.com/en-us/lp/dt/open-manage-idrac.

Actualizaciones automatizadas de firmware y controladores

iDRAC

A diferencia de Supermicro IPMI, Dell iDRAC le permite programar actualizaciones automáticas de firmware. Es decir, configurar actualizaciones automáticas en un programa es una tarea puntual que ahorra tiempo en cada ciclo de actualización. En la figura 5 se muestra el tiempo extrapolado para programar actualizaciones automáticas de firmware por primera vez para 100 servidores con Dell iDRAC y Supermicro IPMI. El proceso manual con la herramienta de Supermicro tarda **13 minutos más** que configurar el proceso automatizado en iDRAC.

Si asumimos que un administrador establece una programación mensual el primer sábado por la noche de cada mes, un administrador que utiliza iDRAC tendría una inversión de tiempo única de 58 segundos por servidor. En el caso de 100 servidores, se trata de una configuración única de 1 hora, 36 minutos y 40 segundos. En comparación, un administrador que utiliza Supermicro IPMI tendría una inversión de 1 hora y 50 minutos para 100 servidores en cada intervalo de mantenimiento. Si comparamos la configuración única de iDRAC y el primero de muchos tiempos de configuración para Supermicro IPMI, la herramienta de gestión de Dell ahorra unos 13 minutos y 20 segundos. (Véase la figura 5).

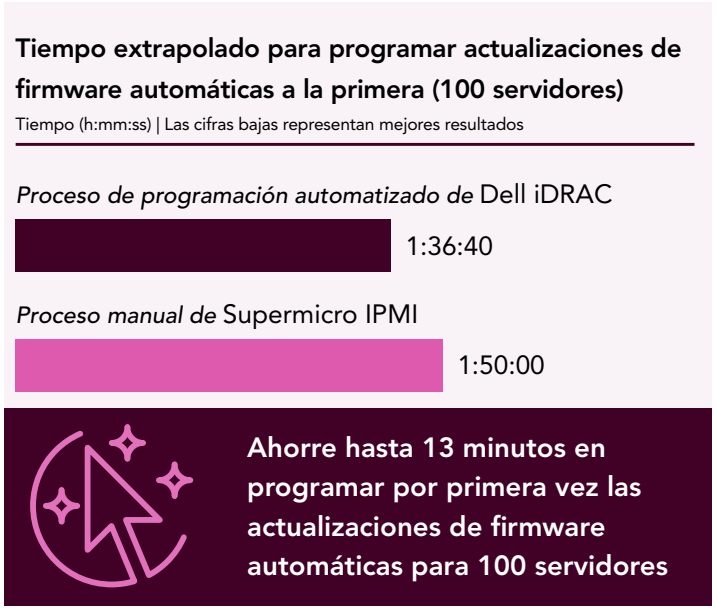

Figura 5: Tiempo extrapolado para actualizar el firmware en 100 servidores la primera vez. Cuanto más bajo es mejor. Fuente: Principled Technologies.

Sin embargo, la segunda vez, y cada vez posterior, **Dell ahorra 110 minutos porque ya no es necesario que el administrador realice la tarea**. (Véase la figura 6). Este ahorro de tiempo se produce incluso si los 100 servidores no están configurados de forma idéntica. Tenga en cuenta que estos tiempos incluyen solo la carga del firmware en BMC y no reflejan los tiempos de descarga y extracción del firmware de Supermicro.

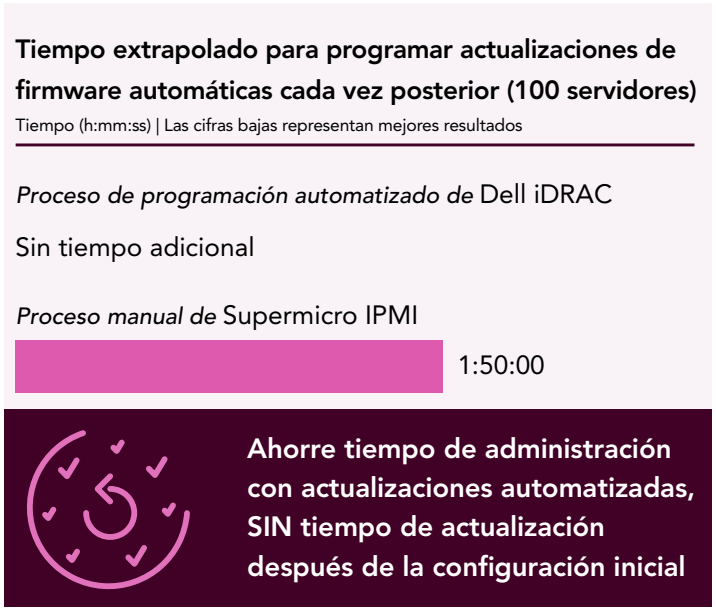

Figura 6: Tiempo extrapolado para actualizar el firmware en 100 servidores en cada vez posterior. Cuanto más bajo es mejor. Fuente: Principled Technologies.

OME

Dell OME admite **actualizaciones de firmware para todos los componentes** y actualizaciones de controladores de Windows. SSM admite la actualización del firmware del BIOS y BMC, pero **no actualizaciones de controladores ni actualizaciones de otros componentes**.

Conclusión

La elección de un proveedor para las compras de servidores implica algo más que solo la plataforma de hardware. Los responsables de la toma de decisiones también deben tener en cuenta las preocupaciones a largo plazo, como la seguridad de los sistemas y los datos, la eficiencia energética y la facilidad de gestión. Estas preocupaciones hacen que las herramientas de gestión de sistemas que ofrece un proveedor sean tan importantes como el hardware.

Investigamos las características y capacidades de las herramientas de gestión de servidores de Dell y Supermicro, comparando Dell iDRAC9 con Supermicro IPMI para la gestión integrada de servidores y Dell OpenManage Enterprise y CloudIQ con Supermicro Server Manager para la gestión y supervisión de dispositivos y consolas de uno a muchos. Descubrimos que las herramientas de gestión de Dell proporcionaban características y capacidades de seguridad, sostenibilidad y gestión/supervisión más completas que los servidores de Supermicro. Además, las herramientas de Dell automatizaron más tareas para facilitar la gestión de servidores, lo que se tradujo en un ahorro significativo de tiempo para los administradores en lugar de tener que hacer las mismas tareas manualmente con las herramientas de Supermicro.

Al realizar una compra de servidores, los productos de gestión asociados a un proveedor son esenciales para proteger los datos, respaldar un entorno más sostenible y facilitar el mantenimiento de los sistemas. Nuestras pruebas e investigaciones mostraron que la cartera de gestión de Dell para servidores PowerEdge ofrecía más funciones para ayudar a las organizaciones a cumplir estos objetivos que los productos de gestión de Supermicro comparables.

1. Steve Morgan, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025", acceso el 15 de febrero de 2024, https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.
2. Dell, "Using iDRAC9 RSA SecurID 2FA", acceso el 15 de febrero de 2024, https://dl.dell.com/Manuals/Common/dellemc-idrac9-rsa-securid-2fa.pdf.
3. Dell, "Dell EMC OpenManage Enterprise SupportAssist Version 1,1 User's Guide", acceso el 15 de febrero de 2024, https://www.dell.com/support/manuals/en-us/openmanage-enterprise-supportassist/omesapuserguide11/role-and-scope-based-access-control-in-openmanage-enterprise?.
4. Dell, "Dell EMC OpenManage Enterprise SupportAssist Version 1.1 User's Guide".
5. Dell, "OpenManage Enterprise 4.0: iDRAC Password Management and Rotation", acceso el 15 de febrero de 2024, https://www.dell.com/support/kbdoc/en-us/000219279/openmanage-enterprise-4-0-idrac-password-management-and-rotation.
6. Dell, "OpenManage Portfolio Software Licensing Guide", acceso el 3 de abril de 2024, https://www.delltechnologies.com/asset/en-us/products/servers/industry-market/openmanage-portfolio-software-licensing-guide.pdf.
7. Mark Maclean y Kyle Shannon, "Dell CloudIQ Cybersecurity for PowerEdge: The Benefits of Automation", acceso el 15 de febrero de 2024, https://infohub.delltechnologies.com/en-US/p/dell-cloudiq-cybersecurity-for-poweredge-the-benefits-of-automation/.
8. Dell, "Security Advisories", acceso el 15 de febrero de 2024, https://infohub.delltechnologies.com/en-US/l/cloudiq-a-detailed-review/security-advisories/.
9. Dell, "Dell CloudIQ - AIOps for Intelligent IT Infrastructure Insights", acceso el 15 de febrero de 2024, https://www.dell.com/en-us/dt/solutions/cloudiq.htm
10. Principled Technologies, "Dell CloudIQ provides a single console for proactive monitoring and had negligible impact on network bandwidth in our tests", acceso el 17 de enero de 2024, https://www.principledtechnologies.com/dell/CloudIQ-network-0422.pdf.
11. Supermicro, "X13DEM User's Manual", acceso el 16 de febrero de 2024, https://www.supermicro.com/manuals/motherboard/X13/MNL-2407.pdf.
12. Dell, "OpenManage Enterprise", acceso el 20 de diciembre de 2023, https://www.dell.com/en-us/work/learn/openmanage-enterprise.
13. Principled Technologies, "A Dell PowerEdge MX environment using OpenManage Enterprise and OpenManage Enterprise Modular can make life easier for administrators", acceso el 17 de enero de 2024, https://www.principledtechnologies.com/Dell/PowerEdge-MX-OME-OME-M-0124.pdf.
14. "Integrated Dell Remote Access Controller (iDRAC)", acceso el 16 de enero de 2024, https://www.dell.com/en-us/lp/dt/open-manage-idrac.

Lea la ciencia detrás de este informe ▶

Principled Technologies®

Facts matter.®

Este proyecto fue encargado por Dell Technologies.

Principled Technologies es una marca comercial registrada de Principled Technologies, Inc.
El resto de los nombres de productos son las marcas comerciales de sus respectivos propietarios.
Para obtener información adicional, consulte los datos científicos sobre los que se fundamenta este informe.