

Dell Command | Monitor Versión 10.0

Guía del usuario



Notas, precauciones y advertencias

 **NOTA:** Una NOTA señala información importante que lo ayuda a hacer un mejor uso de su producto.

 **PRECAUCIÓN:** Una PRECAUCIÓN indica un potencial daño al hardware o pérdida de datos y le informa cómo evitar el problema.

 **ADVERTENCIA:** Una señal de ADVERTENCIA indica la posibilidad de sufrir daño a la propiedad, heridas personales o la muerte.

© 2008 -2018 Dell Inc. o sus filiales. Todos los derechos reservados. Dell, EMC, y otras marcas comerciales son marcas comerciales de Dell Inc. o de sus subsidiarias. Otras marcas pueden ser marcas comerciales de sus respectivos propietarios.

1 Introducción.....	6
Novedades de esta versión.....	6
Descripción general de Dell Command Monitor.....	6
2 Cumplimiento de la Tabla de mitigaciones de seguridad de Windows SMM (WSMT).....	8
3 Características.....	9
Soporte de esquema CIM.....	9
Configuración y enumeración de los ajustes del BIOS.....	9
Seguridad de WMI/OMI.....	9
Creación de informes de alerta.....	10
Apagado remoto.....	10
Acceso a la información del sistema.....	10
Información de propiedad detallada.....	10
Configuración de encendido remoto.....	10
Modificación remota de la configuración del BIOS del sistema.....	10
Estado y condición del sistema.....	10
Supervisión y alertas RAID para controladoras Intel y LSI.....	10
Supervisión y capturas SNMP.....	11
4 Estándares y protocolos.....	12
5 Situaciones de usuarios.....	13
Situación 1: Administración de la propiedad.....	13
Integración SCCM.....	13
Situación 2: Administración de la configuración.....	14
Situación 3: Supervisión de la condición.....	14
Supervisión de alertas del sistema mediante el visor de eventos, syslog o la indicación CIM del sistema operativo.....	14
Situación 4: Perfiles.....	15
Perfil de la batería.....	15
Perfil de administración del BIOS.....	15
Control de inicio.....	15
Base Desktop Mobile.....	15
Escritura en registro.....	16
Propiedad física.....	16
Perfil de memoria del sistema.....	16
6 Uso de Dell Command Monitor.....	17
Configuración del intervalo de sondeo.....	17
Creación de informes del estado RAID.....	17
Supervisión de los sistemas cliente Dell.....	18
Registro de la aplicación de Dell Command Monitor para Linux.....	18

Archivo de configuración.....	18
Detección de unidades de formato avanzado.....	18
Configuraciones de inicio.....	19
DCIM_BootConfigSetting.....	19
DCIM_BootSourceSetting.....	19
DCIM_OrderedComponent.....	19
Cambio de la configuración del sistema.....	20
Configuración de atributos del BIOS en un sistema que ejecuta Windows mediante el uso de comandos PowerShell.....	20
Configuración de los atributos del BIOS en el sistema que ejecuta Linux.....	20
Cambio de la secuencia de inicio.....	23
Apagado y reinicio del sistema Windows de manera remota.....	24
Obtención del valor de la hora del sistema Windows de manera remota.....	24
7 Administración local de sistemas cliente de Dell.....	25
Administración local de sistemas Windows mediante PowerShell.....	25
Administración local de sistemas Linux mediante OMICLI.....	25
8 Administración remota de sistemas cliente de Dell.....	27
Administración de un sistema Windows a través de un sistema Windows de manera remota mediante el uso de PowerShell.....	27
Administración remota del sistema Linux a través del sistema de Windows mediante WinRM.....	27
Administración remota de un sistema Linux a través de un sistema Linux mediante el uso de WSMAN.....	28
9 Preguntas frecuentes.....	29
¿Cómo se encuentra el orden de inicio (secuencia) de la configuración de inicio con la propiedad DCIM_OrderedComponent.AssignedSequence?.....	29
¿Cómo se cambia el orden de inicio?.....	29
¿Cómo se desactivan los dispositivos de inicio?.....	29
Al conectarse con el espacio de nombre con wbemtest, aparece un mensaje de inicio de sesión con error. ¿Cómo se resuelve este problema?.....	29
¿Cómo se ejecutan las secuencias de comandos de TechCenter sin que surjan problemas?.....	29
¿Cómo se establecen los atributos del BIOS?.....	30
¿Dell Command Monitor admite la supervisión del almacenamiento y el sensor para sistemas operativos Windows y Linux?.....	30
¿Puede Dell Command Monitor estar integrado con otras aplicaciones o consolas?.....	30
¿Puedo importar clases en SCCM para el inventario?.....	30
¿Dónde está ubicado el archivo SCCM OMCI_SMS_DEF.mof de la consola SCCM?.....	31
10 Solución de problemas.....	32
No se puede conectar de forma remota al Instrumental de administración de Windows.....	32
Error de instalación en sistemas que ejecutan Windows.....	33
El valor de enumeración de la configuración del BIOS aparece como 1.....	33
No se puede instalar Hapi debido a la dependencia de libsbios.....	34
Recursos CIM no disponibles.....	34
No se pueden ejecutar los comandos mediante DCM en los sistemas que ejecutan Ubuntu Core 16.....	34

11 Otros documentos que puede necesitar.....	35
12 Cómo ponerse en contacto con Dell.....	36
Otros documentos que puede necesitar.....	36
Acceso a documentos desde el sitio de asistencia de Dell EMC.....	36

Introducción

La aplicación del software Dell Command | Monitor activa la administración remota mediante el uso de programas de aplicaciones para acceder a la información, supervisar el estado o cambiar el estado del sistema, como en el caso de apagar el sistema de manera remota. Dell Command | Monitor utiliza los parámetros clave del sistema a través de interfaces estándares, lo que les permite a los administradores gestionar el inventario, supervisar el estado del sistema y recopilar información de los sistemas Dell implementados. Dell Command | Monitor está diseñado para los sistemas cliente de Dell Enterprise y los sistemas Dell de puertos de enlace de IoT, así como para los equipos integrados de Dell. Para obtener más información acerca de los sistemas Dell admitidos, consulte las notas de la versión disponibles en dell.com/dellclientcommandsuitemanuals. En este documento se proporciona una descripción general de Dell Command | Monitor y sus funciones.

NOTA: Dell Command | Monitor era anteriormente Dell OpenManage Client Instrumentation (OMCI). Después de la versión 8.2.1 de OMCI, esta cambió de marca a Dell Command | Monitor.

Temas:

- [Novedades de esta versión](#)
- [Descripción general de Dell Command | Monitor](#)

Novedades de esta versión

Compatibilidad para cumplimiento con WSMT. Para obtener más información sobre el cumplimiento de WSMT, consulte la sección de Cumplimiento de la Tabla de mitigaciones de seguridad de Windows SMM (Windows SMM Security Mitigations Table, WSMT) en la Guía de usuario de Dell Command | Monitor.

Compatibilidad con las siguientes funciones del BIOS:

- Auto Switch, Battery Slice Charge Configuration, BIOS Enumeration Mode, Broadcom TruManage, Dust Filter Maintenance, eMMC, Enable Block SID, Enable Tablet Button LED Sign of Life, Fan Speed Auto Level on Cpu Zone, Fan Speed Auto Level on Psu Zone, GraphicSpecMode, HDD0 Fan Enable, HDD4 Fan Enable, Intel Speed Shift Technology, PCIE0, PCIE1, PCIE0_CPU1, PCIE1_CPU1, PPI Bypass for Block SID Command, PPI Bypass for TPM Clear, Report Logo Type, SATA-8, Secure Boot Mode, SMM Security Mitigation, Slice Battery Custom Charge Limit y Wake on 2nd LAN (RJ-45/SFP).

Para obtener más información sobre los atributos del BIOS, consulte la *Guía de referencia de Dell Command | Monitor* en dell.com/dellclientcommandsuitemanuals.

Descripción general de Dell Command | Monitor

NOTA: El Protocolo simple de administración de red (SNMP) no es compatible con Dell Command | Monitor para Linux.

Dell Command | Monitor administra sistemas cliente mediante el estándar de Modelo de información común (CIM) y el Protocolo simple de administración de red (SNMP), los cuales son protocolos de administración. Esto reduce el costo total de propiedad, mejora la seguridad y ofrece un enfoque integral que administra todos los dispositivos en una red, incluso dispositivos de cliente, servidores, almacenamiento, redes y software.

Con el CIM puede acceder a Dell Command | Monitor a través de los servicios web para los estándares de administración (WSMAN).

Dell Command | Monitor contiene el conjunto de controladores subyacente que recopila información del sistema cliente a partir de varias fuentes distintas, lo que incluye el BIOS, CMOS, el BIOS de administración de sistemas (SMBIOS), la interfaz de administración de sistemas (SMI), el sistema operativo y la interfaz de programación de aplicaciones (API). Dell Command | Monitor para Windows también recopila

información de sistemas cliente de la biblioteca de vínculos dinámicos (DLL) y los ajustes del registro. Dell Command | Monitor para Windows recupera esta información a través de la interfaz de CIM Object Manager (CIMOM), la pila de Windows Management Instrumentation (WMI) o el agente SNMP, mientras que Dell Command | Monitor para Linux recupera esta información a través de la interfaz de Open Management Infrastructure (OMI).

Dell Command | Monitor les permite a los administradores de TI recopilar información de activos de manera remota, modificar la configuración del BIOS, recibir notificaciones proactivas sobre posibles condiciones de error y recibir alertas de posibles vulneraciones de seguridad. En los sistemas que ejecutan Windows, estas alertas se encuentran disponibles como eventos en el registro de eventos de NT, en el evento de WMI o en capturas SNMP v1. Para los sistemas que ejecutan Linux, estas alertas se reciben como un syslog, un evento de OMI o un registro de la aplicación.

Dell Command | Monitor para Windows se puede integrar en una consola como Microsoft System Center Configuration Manager, si se accede directamente a la información de CIM o mediante otros proveedores de consola que hayan implementado la integración de Dell Command | Monitor. Además, se pueden crear secuencias de comandos personalizadas para abordar áreas de interés clave. Existen ejemplos de secuencias de comandos disponibles en la página de Dell TechCenter Dell Command | Monitor. Puede usar estas secuencias de comandos para supervisión del inventario, configuración del BIOS y condición del sistema.

ⓘ **NOTA:** La instalación predeterminada no habilita la compatibilidad SNMP. Para obtener más información acerca de cómo activar la compatibilidad de SNMP para Dell Command | Monitor para Windows, consulte la *Guía de instalación de Dell Command | Monitor* en dell.com/dellclientcommandsuite/manuals.

ⓘ **NOTA:** La instalación predeterminada no habilita la compatibilidad SNMP. Para obtener más información acerca de cómo activar la compatibilidad de SNMP para Dell Command | Monitor para Windows, consulte la *Guía de instalación de Dell Command | Monitor*.

Cumplimiento de la Tabla de mitigaciones de seguridad de Windows SMM (WSMT)

En la tabla de mitigaciones de seguridad de Windows (SMM) se incluye información acerca de la tabla ACPI que se creó para el sistema operativo Windows, la cual admite las funciones de seguridad basadas en la virtualización (VBS) de Windows. Dell Command | Monitor es compatible con WSMT. Se utiliza para configurar las funciones de plataforma en los sistemas cliente de Dell con BIOS con WSMT habilitada.

A continuación, se indican los cambios de comportamiento debido al cumplimiento con WSMT:

- Las funcionalidades de Dell Command | Monitor se encuentran disponibles en las plataformas de cliente de Dell que tengan la versión compatible del BIOS que admita WMI/ACPI. Para obtener más información sobre la lista de plataformas, consulte [Plataformas admitidas](#).

Características

Las funciones clave de Dell Command | Monitor son:

- Soporte de esquema CIM
- Configuración del BIOS
- Seguridad de WMI/OMI
- Informe de sucesos
- Apagado remoto
- Acceso a la información del sistema a través del esquema CIM, mediante el uso del protocolo WSMAN
- Compilación de información de propiedad detallada
- Configurabilidad de encendido remoto
- Modificación remota de la configuración del sistema
- Supervisión de la condición del sistema y el estado de los informes
- Supervisión y alertas RAID para controladoras integradas Intel y controladoras integradas LSI
- Supervisión y excepciones SNMP solo a través de Dell Command | Monitor para Windows

ⓘ | NOTA: Mediante el uso de Dell Command | Monitor para Windows, también se puede acceder a la información a través de SNMP.

ⓘ | NOTA: La supervisión de la controladora integrada Intel no es compatible con los sistemas que ejecutan el sistema operativo Linux.

Soporte de esquema CIM

Dell Command | Monitor para Windows cumple con el esquema CIM 2.17 e incluye dos proveedores de WMI:

- Agente de sondeo o proveedor de indicaciones WMI
- Proveedor de método o instancia WMI

Dell Command | Monitor para Linux cumple con el esquema CIM 2.32.0 e incluye dos proveedores de WMI:

- Agente de sondeo o proveedor de indicaciones WMI
- Proveedor de método o instancia WMI

Configuración y enumeración de los ajustes del BIOS

Dell Command | Monitor ofrece la capacidad de configurar el BIOS del sistema.

Seguridad de WMI/OMI

WMI proporciona la autenticación del usuario antes de otorgar acceso a los datos y métodos CIM. La seguridad del modelo de objeto de componente distribuido (DCOM) y CIMOM aplican los privilegios de acceso. Se puede otorgar acceso completo o limitado a los usuarios según el espacio de nombre. No hay implementación de clases ni seguridad a nivel de la propiedad. De manera predeterminada, los usuarios que son miembros del grupo de administradores tienen acceso remoto y local completo a WMI.

Para Dell Command | Monitor para Windows, puede configurar la seguridad de WMI con el Control de WMI, disponible en la consola de administración del equipo en la sección Servicios y aplicaciones. Haga clic con el botón derecho del mouse en **Control de WMI** y, a continuación, haga clic en **Propiedades**. Puede configurar la seguridad específica del espacio de nombre desde la pestaña **Seguridad**. También puede ejecutar el **Control de WMI** desde el menú **Inicio** o desde la **CLI** ejecutando `wmi.mgmt.msc`.

Creación de informes de alerta

Dell Command | Monitor detecta los eventos en los sistemas Dell y envía alertas al usuario local y al administrador de la red sobre posibles errores, cambios en la configuración, inventario de componentes, controladoras integradas Intel y RAID LSI, sondas e intrusiones en el chasis. Una aplicación de administración de sistemas, como OpenManage Essentials (OME), muestra estos eventos.

Apagado remoto

Dell Command | Monitor para Windows admite el apagado y el reinicio remotos del sistema.

Acceso a la información del sistema

Dell Command | Monitor proporciona acceso a la información del sistema, como la versión del BIOS, el fabricante o proveedor del BIOS, la etiqueta de servicio, el modelo del sistema, la primera fecha de encendido y el modelo del sistema, a través de WMI/OMI con CIM. Además, también se puede utilizar el protocolo WSMAN para acceder a esta información a través de WMI/OMI.

Información de propiedad detallada

Dell Command | Monitor proporciona acceso a información de inventario detallada, como procesadores, memoria, dispositivos PCI y baterías.

Configuración de encendido remoto

Dell Command | Monitor admite la configuración de los ajustes de encendido remoto. El encendido remoto es una función del sistema cliente y la tarjeta de interfaz de red (NIC).

Modificación remota de la configuración del BIOS del sistema

Dell Command | Monitor les permite a los administradores recuperar y establecer la configuración del BIOS del cliente empresarial, como la configuración de puertos USB y la configuración de NIC, etc.

Estado y condición del sistema

Dell Command | Monitor supervisa el estado del sistema, como el estado del ventilador, la memoria, la temperatura, las sondas, la batería, las controladoras RAID y la estación de acoplamiento, e informa sobre su estado.

Supervisión y alertas RAID para controladoras Intel y LSI.

Supervisión y alertas para las unidades físicas y lógicas de las controladoras Intel y RAID LSI para Dell Command | Monitor para Windows; supervisión y alertas solo para controladoras LSI para Dell Command | Monitor para Linux.

En la supervisión de almacenamiento, Dell Command | Monitor admite la supervisión y las alertas de:

- La controladora integrada Intel (compatible con CSMI v0.81 o posterior)
- Las controladoras RAID integradas LSI; y 9217, 9271, 9341, 9361, 9440, 9460 y sus controladores asociados (físicos y lógicos)

NOTA: La supervisión de la controladora integrada Intel no es compatible con los sistemas que ejecutan el sistema operativo Linux.

En la supervisión de sensores, Dell Command | Monitor admite la supervisión y las alertas del voltaje, la temperatura, el amperaje, los dispositivos de enfriamiento (ventilador) y los sensores de chasis.

Supervisión y capturas SNMP

Dell Command | Monitor para Windows es compatible con SNMP v1 y admite la supervisión de los atributos y las excepciones del sistema.

Estándares y protocolos

Dell Command | Monitor se basa en los estándares de CIM. La especificación CIM proporciona detalles sobre técnicas de asignación que ofrecen una mejor compatibilidad con protocolos de administración.

Los protocolos de administración como WMI, SNMP y WSMAN se utilizan para la supervisión remota.

NOTA: Dell Command | Monitor para Windows utiliza el Protocolo simple de administración de red (SNMP) para describir diversas variables del sistema.

El Grupo de tareas de administración de escritorio (DMTF) es la entidad de estándares reconocida por el sector que lidera el desarrollo, la adopción y la unificación de los estándares de administración (incluidos CIM y ASF) y las iniciativas para los entornos empresariales, de escritorio y de Internet.

Situaciones de usuarios

En este capítulo se describen los diversos escenarios de usuarios de Dell Command | Monitor.

Puede utilizar Dell Command | Monitor para:

- [Administración de la propiedad](#)
- [Administración de la configuración](#)
- [Supervisión de la condición](#)
- [Perfiles](#)

Temas:

- [Situación 1: Administración de la propiedad](#)
- [Situación 2: Administración de la configuración](#)
- [Situación 3: Supervisión de la condición](#)
- [Situación 4: Perfiles](#)

Situación 1: Administración de la propiedad

Una empresa que usa muchos sistemas Dell no pudo mantener la información de inventario precisa debido a cambios en el personal del negocio y del departamento de tecnología de la información (TI). El gerente de informática (CIO) solicita un plan para identificar los sistemas que pueden actualizarse a las versiones más recientes de Microsoft Windows. Para ello, se deben evaluar los sistemas implementados a fin de determinar el tamaño, el alcance y el impacto financiero de dicho proyecto. La recopilación de información supone un esfuerzo importante. Asignar personal de TI para cada sistema cliente es costoso en términos de horas hombre e interrupciones de los usuarios finales.

Mediante el uso de Dell Command | Monitor en cada sistema Dell, el administrador de TI puede recopilar rápidamente información de forma remota. Mediante herramientas como Microsoft System Center Configuration Manager (SCCM), el administrador de TI realiza consultas sobre cada sistema cliente a través de la red y recopila información como el tipo de CPU y su velocidad, el tamaño de la memoria, la capacidad de unidad de disco duro, la versión del BIOS y la versión del sistema operativo actual. Una vez recopilada esta información, es posible analizarla para identificar los sistemas que se pueden actualizar a las versiones más recientes de Windows.

También es posible obtener el inventario de activos a través de la línea de comandos de WSMAN/WinRM o utilizando cualquier línea de comandos de cliente CIM.

Integración SCCM

Es posible integrar SCCM con Dell Command | Monitor para Windows mediante:

- El uso del archivo MOF incluido en el paquete de instalación de Dell Command | Monitor, que contiene todas las clases de Dell Command | Monitor y su importación a ConfigMgr

El archivo MOF se encuentra en:

`C:\Program Files\Dell\Command_Monitor\ssa\omacim\OMCI_SMS_DEF.mof`

- La extensión de las capacidades de creación de informes de propiedad mediante el uso de colecciones.

Situación 2: Administración de la configuración

Una compañía planea estandarizar la plataforma del cliente y administrar cada sistema a través de su ciclo de vida. Como parte de este esfuerzo, la empresa adquiere un conjunto de herramientas y planea automatizar la implementación de un sistema operativo del cliente nuevo con el Entorno de ejecución previa al inicio (PXE).

El desafío es modificar la contraseña del BIOS en el BIOS de cada equipo cliente sin visitar manualmente el escritorio. Con Dell Command | Monitor instalado en cada sistema cliente, el departamento de TI de la empresa dispone de varias opciones para modificar de forma remota el orden de inicio. OpenManage Essentials (OME) es una consola de administración que se puede integrar con Dell Command | Monitor y que se puede utilizar para supervisar la configuración del BIOS de manera remota en todos los sistemas cliente empresariales. Otra opción es escribir una secuencia de comandos (CIM, WinRM/WSMAN/PowerShell/WMIC) que cambie la configuración del BIOS. La secuencia de comandos se puede proporcionar de manera remota a través de la red y ejecutarse en cada sistema cliente.

Para obtener más información acerca de Dell Command | Monitor, consulte la *Guía de referencia de Dell Command | Monitor* en dell.com/dellclientcommandssuitemanuals.

Para obtener más información acerca de Dell Command | Monitor, consulte la *Dell Command | Monitor*.

Las configuraciones estandarizadas pueden proporcionar ahorros de costos considerables para las empresas de todas las envergaduras. Muchas organizaciones implementan sistemas cliente estandarizados, pero solo unas pocas administran la configuración del sistema durante toda la vida útil de la computadora. Con Dell Command | Monitor instalado en cada sistema cliente, el departamento de TI puede bloquear los puertos heredados para evitar el uso de periféricos no autorizados o habilitar Wake On LAN (WOL) para que el sistema pueda reactivarse de un estado de inactividad durante las horas no pico con el fin de realizar tareas de administración de sistemas.

Situación 3: Supervisión de la condición

Un usuario recibe mensajes de error de lectura mientras intenta acceder a determinados archivos en el disco duro del sistema cliente. El usuario reinicia el sistema y ahora puede acceder a los archivos. El usuario ignora el problema inicial, porque parece haberse solucionado solo. Mientras tanto, Dell Command | Monitor consulta el problema de una falla prevista en la unidad de disco duro y envía una alerta de Tecnología de supervisión automática, análisis y generación de informes (SMART) a la consola de administración. También le muestra el error de SMART al usuario local. La alerta indicó que están ocurriendo varios errores de lectura o escritura en el disco duro. El departamento de TI de la empresa le recomendó al usuario realizar inmediatamente un respaldo de los archivos con datos importantes. Se envía a un técnico de servicio con una unidad de reemplazo.

Se reemplaza la unidad de disco duro antes de que se produzca el error, lo que evita el tiempo de inactividad del usuario, una llamada al servicio de asistencia y un viaje del técnico hasta el escritorio para diagnosticar el problema.

Supervisión de alertas del sistema mediante el visor de eventos, syslog o la indicación CIM del sistema operativo

Dell Command | Monitor admite la supervisión de eventos a través de los siguientes procedimientos:

- Transmisión del registro a través de la clase CIM **DCIM_LogEntry**.
- Supervisión de la indicación CIM a través de la clase **DCIM_AlertIndication**.
- (solo para Dell Command | Monitor para Windows) Supervisión de eventos a través del Protocolo simple de administración de red (SNMP) y el visor de eventos de Windows.
- (solo para Dell Command | Monitor para Linux) Supervisión mediante syslog.

Para obtener más información acerca de Dell Command | Monitor, consulte la *Guía de referencia de Dell Command | Monitor* en dell.com/dellclientcommandssuitemanuals.

Para obtener más información acerca de Dell Command | Monitor, consulte la *Dell Command | Monitor*.

Situación 4: Perfiles

NOTA: Los perfiles de DMTF se implementan solo en Dell Command | Monitor para Windows.

Los administradores de TI deben controlar los sistemas cliente en entornos empresariales distribuidos y de múltiples proveedores. Se enfrentan con numerosos desafíos, ya que deben dominar un conjunto diverso de herramientas y aplicaciones, y al mismo tiempo administrar varios sistemas cliente móviles y de escritorio en diferentes redes. Para reducir el costo de estos requisitos y representar los datos de administración proporcionados, se implementan los perfiles de Grupo de trabajo de administración distribuida (DMTF) y de Administración de infraestructura de centros de datos (DCIM-OEM) estándar del sector en Dell Command | Monitor. Algunos de los perfiles de DMTF se explican en esta guía.

Para obtener más información acerca de Dell Command | Monitor, consulte la *Guía de referencia de Dell Command | Monitor* en dell.com/dellclientcommandsuite/manuals.

Para obtener más información acerca de Dell Command | Monitor, consulte la *Guía de referencia de Client Command | Monitor*.

Perfil de la batería

- Determine el estado de la batería al enumerar u obtener la instancia de la clase **DCIM_Battery**.
- Determine la hora de ejecución estimada y vea la carga restante estimada.
- Compruebe si la información de condición de la batería se puede determinar mediante las propiedades *OperationalStatus* y *HealthState* de la clase **DCIM_Battery**.
- Obtenga información adicional sobre la condición de una batería mediante la propiedad **DCIM_Sensor.CurrentState** o **CIM_NumericSensor.CurrentState**.

Perfil de administración del BIOS

- Determine la versión del BIOS. Para ello, enumere la instancia de la clase **DCIM_BIOSElement**.
- Verifique si los valores del atributo del BIOS se pueden modificar o no. Obtenga la instancia de la clase **DCIM_BIOSEnumeration**. El atributo puede modificarse si la propiedad **IsReadOnly** está establecida en FALSO.
- Configure la contraseña del sistema (SystemPwd). Ejecute el método **DCIM_BIOSService.SetBIOSAttributes()** y establezca SystemPwd en AttributeName y el valor de contraseña en los parámetros de AttributeValue.
- Establezca la contraseña del BIOS o administración (AdminPwd). Ejecute el método **DCIM_BIOSService.SetBIOSAttributes()** y establezca AdminPwd en AttributeName y el valor de contraseña en los parámetros de AttributeValue.
- Ejecute el método **DCIM_BIOSService.SetBIOSAttributes()** y especifique los parámetros AttributeName y AttributeValue.
- Para modificar un atributo del BIOS cuando se establece la contraseña del administrador o del BIOS, ejecute el método **DCIM_BIOSService.SetBIOSAttributes()** y especifique los valores AttributeName, AttributeValue y la contraseña del BIOS actual en el parámetro de entrada AuthorizationToken.

Control de inicio

- Cambie la secuencia de los elementos de inicio en la lista de inicio heredada y de UEFI.
- Active o desactive los elementos de inicio de la lista de inicio heredada y de UEFI.
- Busque la configuración de inicio actual enumerando las instancias de la clase **DCIM_ElementSettingData** cuya propiedad **IsCurrent** está establecida en 1. **DCIM_BootConfigSetting** representa la configuración de inicio actual.

Base Desktop Mobile

- Determine el modelo de sistema, la etiqueta de servicio y el número de serie. Para ello, enumere la instancia de la clase **DCIM_ComputerSystem**.

- Ejecute el método **DCIM_ComputerSystem.RequestStateChange()** y establezca el valor del parámetro RequestedState en **3**. Apague el sistema.
- Reinicie el sistema. Ejecute el método **DCIM_ComputerSystem.RequestStateChange()** y establezca el valor del parámetro **RequestedState** en **11**.
- Determine el estado de la alimentación del sistema.
- Determine la cantidad de procesadores en el sistema. Para ello, realice consultas en **DCIM_Processor**, instancias que se asocian con la instancia central mediante la asociación **DCIM_SystemDevice**.
- Obtenga la hora del sistema. Ejecute el método **DCIM_TimeService.ManageTime()** y establezca el parámetro **GetRequest** en **Verdadero**.
- Compruebe la condición del elemento administrado.

Escritura en registro

- Para identificar el nombre del registro, seleccione la instancia **DCIM_RecordLog** en la que la propiedad **ElementName** corresponde al nombre del registro.
- Busque las entradas de registros individuales. Obtenga todas las instancias de **DCIM_LogEntry** que están asociadas con la instancia especificada de **DCIM_RecordLog** a través de la asociación **DCIM_LogManagesRecord**. Ordene las instancias en función de **RecordID**.
- Verifique si las escrituras en registro están activadas o no al enumerar la instancia de la clase **DCIM_RecordLog** cuya propiedad **Enabledstate** está establecida en **2** (que representa Activado) y **EnabledState** está establecida en **3** (que representa Desactivado).
- Clasifique los registros según la hora de la entrada del registro. Obtenga todas las instancias de **DCIM_LogEntry** que están asociadas con la instancia especificada de **DCIM_RecordLog** a través de la asociación **DCIM_LogManagesRecord**. Clasifique las instancias de **DCIM_LogEntry** en función del valor de la propiedad **CreationTimeStamp** en el orden "último en entrar, primero en salir" (Last In First Out, LIFO).
- Borre los registros. Para ello, ejecute el método **ClearLog()** para la instancia determinada de **DCIM_RecordLog**.

Propiedad física

- Obtenga el inventario físico de todos los dispositivos de un sistema.
- Obtenga el inventario físico para el chasis de un sistema.
- Determine el número de pieza de un componente fallado.
- Determine si la ranura está vacía o no.

Perfil de memoria del sistema

- Obtenga la información de la memoria del sistema.
- Obtenga la información de la memoria física del sistema.
- Compruebe el tamaño de la memoria del sistema.
- Compruebe el tamaño de la memoria del sistema disponible.
- Compruebe el tamaño de la memoria física del sistema.
- Compruebe el estado de la condición de la memoria del sistema.

Uso de Dell Command | Monitor

Puede ver la información que proporciona Dell Command | Monitor accediendo a:

- `root\dcim\sysman (standard)`

Dell Command | Monitor proporciona la información a través de clases en estos espacios de nombre.

Para obtener más información sobre las clases, consulte la *Guía de referencia de Dell Command | Monitor* en dell.com/dellclientcommandsuite manuals.

Para obtener más información sobre las clases, consulte la *Guía de referencia de Dell Command | Monitor*.

Temas:

- Configuración del intervalo de sondeo
- Creación de informes del estado RAID
- Supervisión de los sistemas cliente Dell
- Registro de la aplicación de Dell Command | Monitor para Linux
- Detección de unidades de formato avanzado
- Configuraciones de inicio
- Cambio de la configuración del sistema

Configuración del intervalo de sondeo

Puede cambiar el intervalo de sondeo de la sonda del ventilador, de la sonda de temperatura, de la sonda de voltaje, de la sonda de corriente, del aumento o disminución de la capacidad del disco, del aumento o disminución del tamaño de la memoria y del aumento o disminución de la cantidad de procesadores con Dell Command | Monitor.

- Para Windows, el archivo `dcsbdy32.ini` o `dcsbdy64.ini` se encuentra en `<ubicación de instalación de Dell Command | Monitor>\omsa\ini`.
- Para Linux, el archivo `AlertPollingSettings.ini` se encuentra en `/opt/dell/dcm/conf`.

NOTA: Los números del archivo INI son múltiplos de 23. El intervalo de sondeo predeterminado para la capacidad de disco y la alerta de Tecnología de autosupervisión, análisis e informes (SMART) es 626 segundos (el tiempo real = 626 x 23 segundos, que equivale a aproximadamente 3 horas).

Creación de informes del estado RAID

Dell Command | Monitor habilita la información de la configuración de RAID y supervisa la funcionalidad de RAID para los sistemas cliente con compatibilidad de hardware y controlador. Se pueden utilizar las clases RAID para obtener detalles sobre niveles RAID, información sobre el controlador, configuración de la controladora y estado de la controladora. Una vez activada la configuración de RAID, es posible recibir alertas sobre la degradación o falla de los controladores y las controladoras.

NOTA: La creación de informes del estado RAID se admite solo para las controladoras RAID que trabajan en controladores compatibles con Common Storage Management Interface (CSMI) versión 0.81. Las versiones OMCI 8.1 y posteriores admiten la supervisión solo en las controladoras RAID en chips de Intel, y las versiones OMCI 8.2 y posteriores admiten alertas para controladoras RAID en chips de Intel.

Supervisión de los sistemas cliente Dell

- Dell Command | Monitor para Windows admite el Protocolo simple de administración de red (SNMP) para la supervisión y administración de sistemas cliente tales como equipos portátiles, equipos de escritorio y estaciones de trabajo. El archivo de la Base de información de administración (MIB) se comparte entre Dell Command | Monitor y Server Administrator. Se ha modificado Dell Command | Monitor para Windows desde la versión 9.0 para utilizar un OID específico para el OID del cliente (10909) para que las consolas identifiquen los sistemas cliente.

Para obtener más información sobre SNMP, consulte la *Guía de referencia de SNMP de Dell Command | Monitor* en dell.com/dellclientcommandsuite/manuals.

Para obtener más información sobre SNMP, consulte la *Guía de referencia de SNMP de Dell Command | Monitor*.

- Dell Command | Monitor para Linux admite la supervisión mediante el uso de comandos de WinRM y WSMAN.

Registro de la aplicación de Dell Command | Monitor para Linux

Dell Command | Monitor para Linux segrega los registros y alertas de la aplicación para fines de creación de informes y depuración. El historial de las alertas y los registros generados para la aplicación Dell Command | Monitor pueden ser vistos en el archivo **dcm_application.log** disponible en `/opt/dell/dcm/var/log`.

Archivo de configuración

Puede actualizar el archivo de configuración **log.property** disponible en `/opt/dell/dcm/conf` para aplicar la configuración deseada y realizar la DEPURACIÓN:

① **NOTA: Reinicie el servidor OMI después de realizar cualquier cambio en el archivo de configuración para aplicar los cambios.**

- **Log_Level:** existen tres niveles de registro para separar los mensajes del sistema: ERROR, INFORMACIÓN y DEPURACIÓN

El usuario puede cambiar el nivel de registro del archivo de configuración. Si el nivel de registro se establece en DEPURAR, el registro de la aplicación Dell Command | Monitor enviará toda la información en el archivo de registro especificado.

① **NOTA: El nivel de registro predeterminado está establecido en INFORMACIÓN.**

- **File_Size:** el usuario puede especificar el tamaño máximo del archivo **dcm_application.log**. El tamaño predeterminado del archivo es de 500 MB.

① **NOTA: El valor de File_Size debe ser expresado en bytes.**

- **BackupIndex:** el usuario puede especificar el conteo de sustitución de **dcm_application.log**. Si el conteo de sustitución predeterminado es de 2, el tercer archivo de respaldo reemplazará al archivo más antiguo.

Detección de unidades de formato avanzado

Los sistemas cliente están en transición a unidades de formato avanzado (AF) para proporcionar mayor capacidad de almacenamiento y para abordar las limitaciones de las unidades de disco duro (HDD) de 512 bytes. Los discos duros en transición a sectores de 4KB conservan la compatibilidad inversa, mientras que el disco duro de formato avanzado actual, también conocido como disco duro de 512e, es compatible con SATA de 512 bytes y opera a 4KB. Durante la transición, es posible que experimente problemas de rendimiento, como unidades de partición desalineadas en los sistemas cliente, que provocan fallas de los paquetes de software de cifrado basados en sectores que manejan unidades de 512e. Dell Command | Monitor le permite determinar si la unidad de disco duro de un sistema es una unidad de formato avanzado de 4KB, lo que ayuda a evitar estos problemas.

Configuraciones de inicio

NOTA: Dell Command | Monitor para Linux no ofrece las funcionalidades de configuración de inicio. Por lo tanto, esta sección no es aplicable para Dell Command | Monitor para Linux.

Un sistema cliente puede tener uno de los dos tipos de configuración de inicio:

- Heredada (BIOS)
- UEFI

En Dell Command | Monitor, la configuración de inicio (heredada o UEFI) se modela con las siguientes clases:

- **DCIM_ElementSettingData**
- **DCIM_BootConfigSetting**
- **DCIM_OrderedComponent**
- **DCIM_BootSourceSetting**

NOTA: Los términos "Configuración de inicio" y "Tipo de lista de inicio" se utilizan indistintamente y tienen el mismo significado ya sea que representen Heredada o UEFI.

DCIM_BootConfigSetting

Una instancia de **DCIM_BootConfigSetting** representa una configuración de inicio que se utiliza durante el proceso de inicio. Por ejemplo, en los sistemas cliente, existen dos tipos de configuraciones de inicio: heredada y UEFI. Por lo tanto, **DCIM_BootConfigSetting** tiene un máximo de dos instancias que representan, una para la configuración heredada y otra para UEFI.

Puede determinar si **DCIM_BootConfigSetting** representa Heredada con las siguientes propiedades:

- InstanceID = "DCIM:BootConfigSetting:Next:1"
- ElementName = "Next Boot Configuration Setting : Boot List Type 1"

Puede determinar si **DCIM_BootConfigSetting** representa UEFI con las siguientes propiedades:

- InstanceID = "DCIM:BootConfigSetting:Next:2"
- ElementName = "Next Boot Configuration Setting : Boot List Type 2"

DCIM_BootSourceSetting

Esta clase representa las fuentes o los dispositivos de arranque. Las propiedades **ElementName**, **BIOSBootString** y **StructuredBootString** contienen una cadena que identifica los dispositivos de arranque. Por ejemplo, disco flexible, disco duro, CD/DVD, red, Asociación Internacional de Tarjetas de Memoria para Computadoras Personales, Vehículo eléctrico de batería o USB. Según el tipo de lista de inicio del dispositivo, una instancia de **DCIM_BootSourceSetting** está asociada con una de las instancias de **DCIM_BootConfigSetting**.

DCIM_OrderedComponent

La clase de la asociación **DCIM_OrderedComponent** se usa para asociar las instancias de **DCIM_BootConfigSetting** con instancias de **DCIM_BootSourceSetting** que representan uno de los tipos de lista de inicio (heredada o UEFI) a los que pertenecen los dispositivos de inicio. La propiedad **GroupComponent** de **DCIM_OrderedComponent** se refiere a la instancia **DCIM_BootConfigSetting** y la propiedad **PartComponent** se refiere a la instancia **DCIM_BootSourceSetting**.

Cambio de la configuración del sistema

En Dell Command | Monitor, utilice los siguientes métodos para cambiar la configuración del sistema y el estado de los sistemas locales o remotos:

- **SetBIOSAttributes:** cambia la configuración del BIOS
 - ① **NOTA:** Dell Command | Monitor para Linux actualmente solo admite el método SetBIOSAttributes.
- **ChangeBootOrder:** cambia la configuración de inicio
- **RequestStateChange:** apaga y reinicia el sistema
- **ManageTime:** muestra la hora del sistema

En Dell Command | Monitor para Windows, puede ejecutar estos métodos con winrm, secuencias de comandos VB, comandos PowerShell, wmic y WMI wbemtest.

Configuración de atributos del BIOS en un sistema que ejecuta Windows mediante el uso de comandos PowerShell

Puede establecer los atributos del BIOS con el método SetBIOSAttributes. El procedimiento se explica a continuación mediante una tarea para habilitar el Módulo de plataforma segura (TPM) como ejemplo.

① **NOTA:** Asegúrese de que la opción TPM está desactivada en el BIOS antes de seguir el procedimiento para activar el TPM.

① **NOTA:** Utilice PowerShell con privilegios de administrador.

Para habilitar TPM:

- 1 Configure la contraseña del BIOS en el sistema si ya no está configurada con el siguiente comando de PowerShell:

```
Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSService | Invoke-CimMethod -Method Name SetBIOSAttributes -Arguments @{AttributeName=@("AdminPwd");AttributeValue=@("<Admin password>")}
```
- 2 Active la seguridad de TPM con el siguiente comando:

```
Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSService | Invoke-CimMethod -Method Name SetBIOSAttributes -Arguments @{AttributeName=@("Trusted Platform Module");AttributeValue=@("1");AuthorizationToken="<Admin password>"}
```
- 3 Reinicie el sistema.
- 4 Active el TPM con el siguiente comando:

```
Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSService | Invoke-CimMethod -Method Name SetBIOSAttributes -Arguments @{AttributeName=@("Trusted Platform Module Activation");AttributeValue=@("2");AuthorizationToken="<Admin password>"}
```
- 5 Reinicie el sistema.

Configuración de los atributos del BIOS en el sistema que ejecuta Linux

Puede establecer los atributos del BIOS utilizando cualquiera de los siguientes métodos:

- [Uso de OMICLI](#)
- [Uso de WinRM](#)
- [Uso de WSMAN](#)

NOTA: Asegúrese de que el servidor OMI esté en ejecución.

Configuración de atributos del BIOS mediante el uso de OMICLI

Puede establecer los atributos del BIOS con el método SetBIOSAttributes. El procedimiento se explica a continuación mediante una tarea para habilitar el Módulo de plataforma segura (TPM) como ejemplo.

NOTA: Asegúrese de que la opción TPM está desactivada en el BIOS antes de seguir el procedimiento para activar el TPM.

Para establecer los atributos del BIOS con comandos de OMICLI:

- 1 Para establecer la contraseña del BIOS en el sistema, si es que no está establecida ya, ejecute

```
./omicli iv root/dcim/sysman { DCIM_BIOSService Name DCIM:BiosService  
SystemCreationClassName DCIM_ComputerSystem SystemName <system name displayed in  
DCIM_BIOSService class> CreationClassName DCIM_BIOSService } SetBIOSAttributes  
{ AttributeName "AdminPwd" AttributeValue "<new Admin Password>" }
```

- 2 Para habilitar la seguridad de TPM, utilice el siguiente comando y ejecute

```
./omicli iv root/dcim/sysman { DCIM_BIOSService Name DCIM:BiosService  
SystemCreationClassName DCIM_ComputerSystem SystemName <system name displayed in  
DCIM_BIOSService class> CreationClassName DCIM_BIOSService } SetBIOSAttributes  
{ AttributeName "Trusted Platform Module" AttributeValue "1" AuthorizationToken "<password>" }
```

- 3 Reinicie el sistema.

- 4 Para activar el TPM, ejecute

```
./omicli iv root/dcim/sysman { DCIM_BIOSService Name DCIM:BiosService  
SystemCreationClassName DCIM_ComputerSystem SystemName <system name displayed in  
DCIM_BIOSService class> CreationClassName DCIM_BIOSService } SetBIOSAttributes  
{ AttributeName "Trusted Platform Module Activation" AttributeValue "2" AuthorizationToken  
"<password>" }
```

- 5 Reinicie el sistema.

- 6 Para restablecer la contraseña del BIOS, ejecute

```
./omicli iv root/dcim/sysman { DCIM_BIOSService Name DCIM:BiosService  
SystemCreationClassName DCIM_ComputerSystem SystemName <system name displayed in  
DCIM_BIOSService class> CreationClassName DCIM_BIOSService } SetBIOSAttributes  
{ AttributeName "AdminPwd" AttributeValue "" AuthorizationToken "<password>" }
```

Configuración de atributos del BIOS mediante el uso de WinRM

Puede establecer los atributos del BIOS con el método SetBIOSAttributes. El procedimiento se explica a continuación mediante una tarea para habilitar el Módulo de plataforma segura (TPM) como ejemplo. Para obtener información más detallada, consulte [Administración remota de sistemas cliente de Dell](#).

NOTA: Asegúrese de que la opción TPM está desactivada en el BIOS antes de seguir el procedimiento para activar el TPM.

Para establecer los atributos del BIOS con comandos de WinRM:

- 1 Establezca el selector detallando la clase DCIM_BIOSService. Ejecución:

```
winrm e wsman/DCIM_BIOSService?__cimnamespace=root/dcim/sysman -auth:basic -r:https://  
<system IP or system name>:<Port Number (5985/5986)> -username:<user name> -  
password:<password> -skipCAcheck -skipCNcheck -encoding:utf-8 -returnType:epr
```

NOTA: Los valores establecidos del selector (SystemName=<nombre del sistema de la clase DCIM_BIOSService>winrm i SetBIOSAttributes wsman/DCIM_BIOSService?SystemName=dt: +SystemCreationClassName=DCIM_ComputerSystem +Name=DCIM:BiosService+CreationClassName=DCIM_BIOSService+) serán utilizados para la operación establecida en este ejemplo.

- 2 Configure la contraseña del BIOS en el sistema si ya no está configurada con el siguiente comando:

```
winrm i SetBIOSAttributes http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_BIOSService?  
__cimnamespace=root/dcim/sysman+Name=DCIM:BiosService  
+SystemCreationClassName=DCIM_ComputerSystem+SystemName=<system name from DCIM_BIOSService
```

```
class>+CreationClassName=DCIM_BIOSService -r:https://<system IP or system name>:5986 -u:<user name> -password:<password> -auth:basic -skipCAcheck -skipCNcheck -encoding:utf-8 @<AttributeName="AdminPwd";AttributeValue="<Password">}
```

- 3 Active la seguridad de TPM ejecutando el siguiente comando:

```
winrm i SetBIOSAttributes "http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_BIOSService?__cimnamespace=root/dcim/sysman+Name=DCIM:BiosService +SystemCreationClassName=DCIM_ComputerSystem+SystemName=<system name from DCIM_BIOSService class>+CreationClassName=DCIM_BIOSService -r:https://<system IP or system name>:5986 -u:<user name> -password:<password> -auth:basic -skipCAcheck -skipCNcheck -encoding:utf-8 @<AttributeName="Trusted Platform Module";AttributeValue="1";AuthorizationToken="<Admin password">}"
```

- 4 Reinicie el sistema.

- 5 Active el TPM con el siguiente comando:

```
winrm i SetBIOSAttributes "http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_BIOSService?__cimnamespace=root/dcim/sysman+Name=DCIM:BiosService +SystemCreationClassName=DCIM_ComputerSystem+SystemName=<system name from DCIM_BIOSService class>+CreationClassName=DCIM_BIOSService -r:https://<system IP or system name>:5986 -u:<user name> -password:<password> -auth:basic -skipCAcheck -skipCNcheck -encoding:utf-8 @<AttributeName="Trusted Platform Module Activation";AttributeValue="2";AuthorizationToken="<Admin password">}"
```

Configuración de atributos del BIOS mediante el uso de WSMAN

Puede establecer los atributos del BIOS en los sistemas que ejecutan Linux mediante WSMAN. El procedimiento se explica a continuación mediante una tarea para habilitar el Módulo de plataforma segura (TPM) como ejemplo. Para obtener información más detallada, consulte [Administración remota de sistemas cliente de Dell](#).

ⓘ | NOTA: Asegúrese de que la opción TPM está desactivada en el BIOS antes de seguir el procedimiento para activar el TPM.

- 1 Establezca el selector detallando la clase DCIM_BIOSService. Ejecución:

```
wsman invoke -a "SetBIOSAttributes" http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_BIOSService?Name="DCIM:BIOSService", SystemCreationClassName="DCIM_ComputerSystem", SystemName="<system name from DCIM_BIOSService class>", CreationClassName="DCIM_BIOSService" -N root/dcim/sysman -h <system IP/name> -P 5985 -u <user name> -p <password> -y basic -v -V -k "AttributeName=AdminPwd" -k "AttributeValue=<password>"
```

- 2 Configure la contraseña del BIOS en el sistema si ya no está configurada con el siguiente comando:

```
wsman invoke -a "SetBIOSAttributes" http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_BIOSService?Name="DCIM:BIOSService", SystemCreationClassName="DCIM_ComputerSystem", SystemName="<system name from DCIM_BIOSService class>", CreationClassName="DCIM_BIOSService" -N root/dcim/sysman -h <system IP or system name> -P 5985 -u <user name> -p <password> -y basic -v -V -k "AttributeName=Trusted Platform Module" -k "AttributeValue=1" -k "AuthorizationToken=<password>"
```

- 3 Active la seguridad de TPM con el siguiente comando:

```
wsman invoke -a "SetBIOSAttributes" http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_BIOSService?Name="DCIM:BIOSService", SystemCreationClassName="DCIM_ComputerSystem", SystemName="<system name from DCIM_BIOSService class>", CreationClassName="DCIM_BIOSService" -N root/dcim/sysman -h <system IP or system name> -P 5985 -u <user name> -p <password> -y basic -v -V -k "AttributeName=Trusted Platform Module Activation" -k "AttributeValue=2" -k "AuthorizationToken=<password>"
```

- 4 Reinicie el sistema.

- 5 Active el TPM con el siguiente comando:

```
wsman invoke -a "SetBIOSAttributes" http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_BIOSService?Name="DCIM:BIOSService", SystemCreationClassName="DCIM_ComputerSystem", SystemName="<system name from DCIM_BIOSService class>", CreationClassName="DCIM_BIOSService" -N root/dcim/sysman -h <system IP/name> -P 5985 -u <user name> -p <password> -y basic -v -V -k "AttributeName=AdminPwd" -k "AttributeValue=" -k "AuthorizationToken=<password>"
```

Cambio de la secuencia de inicio

Para cambiar la secuencia de inicio, siga los pasos que se indican a continuación:

:

- 1 **Compruebe el tipo de orden de inicio (heredado o UEFI) usando el siguiente comando:**

- Comando de WMIC: `wmic /namespace:\\root\dcim\sysman path dcim_BootConfigSetting get ElementName/format:list.`
- Comando de PowerShell: `gwmi -namespace root\dcim\sysman -class dcim_BootConfigSetting -Property ElementName.`

- 2 **Compruebe el tipo de orden de inicio (heredado o UEFI) actual usando el siguiente comando:**

- Comando de WMIC: `wmic /namespace:\\root\dcim\sysman path dcim_ElementSettingData.IsCurrent=1 get SettingData /format:list .`
- Comando de PowerShell: `gwmi -namespace root\dcim\sysman -class dcim_elementSettingData -Filter "IsCurrent=1" -Property SettingData.`

- 3 **Cambio de orden de inicio usando el siguiente comando:**

- Comando de WMIC: `wmic /namespace:\\root\dcim\sysman path dcim_bootconfigsetting call ChangeBootOrder /?:full .`
- Comando de PowerShell: `(gwmi -namespace root\dcim\sysman -class dcim_bootconfigsetting).getmethodparameters("ChangeBootOrder") .`

ⓘ **NOTA:** La instancia `dcim_BootConfigSetting` debe representar la configuración de inicio que desea cambiar, ya sea de tipo 1 (heredada) o de tipo 2 (UEFI).

- Los argumentos son:
 - `Authorization Token`: esta es la contraseña de inicio o de administrador.
 - `Source`: esta es la lista de orden de inicio extraída de la propiedad `dcim_OrderedComponent.PartComponent`. El nuevo orden de inicio está determinado por el orden de los dispositivos de inicio en el arreglo de discos de origen.

- 4 **Cambio del orden de inicio para la lista de inicio de tipo 1 con PowerShell:**

- a Obtenga el orden de inicio actual para la lista de inicio de tipo 1 ejecutando el siguiente comando: `$boLegacy = gwmi -namespace root\dcim\sysman -class dcim_orderedcomponent | where {$_.partcomponent -match 'BootListType-1'} | select -expand partcomponent.`
- b Defina una variable PowerShell para especificar el orden de inicio para establecer `$newboLegacy`. Asigne el nuevo orden de inicio a esta variable. Por ejemplo, se conserva el tipo de orden de inicio actual.
- c `$newboLegacy = $boLegacy`
- d Obtenga la instancia `dcim_bootconfigsetting` correspondiente a la lista de inicio de tipo 1 ejecutando el siguiente comando: `$bcsLegacy = Gwmi -Namespace root\dcim\sysman -ClassName dcim_bootconfigsetting | where {$_.ElementName -eq 'Next Boot Configuration Setting : Boot List Type 1'}.`
- e Invoque el método ejecutando el siguiente comando: `$ bcsLegacy.changebootorder($newboLegacy, $AuthorizationToken)`. La variable `$AuthorizationToken` se utiliza para aprobar la contraseña del BIOS.

- 5 **Cambio del orden de inicio para la lista de inicio de tipo 2 con PowerShell:**

- a Obtenga el orden de inicio actual para la lista de inicio de tipo 2 ejecutando el siguiente comando: `$boUefi = gwmi -namespace root\dcim\sysman -class dcim_orderedcomponent | where {$_.partcomponent -match 'BootListType-2'} | select -expand partcomponent.`
- b Defina una variable de PowerShell para especificar el orden de inicio para establecer `$newboUefi`. Asigne el nuevo orden de inicio a esta variable. Por ejemplo, se conserva el tipo de orden de inicio actual.
- c Obtenga la instancia `dcim_bootconfigsetting` correspondiente a la lista de inicio de tipo 2 ejecutando el siguiente comando: `$bcsUefi = Gwmi -Namespace root\dcim\sysman -ClassName dcim_bootconfigsetting | where {$_.ElementName -eq 'Next Boot Configuration Setting : Boot List Type 2'}.`
- d Invoque el método ejecutando el siguiente comando: `$ bcsUefi.changebootorder($newboUefi, $AuthorizationToken)`. La variable `$AuthorizationToken` se utiliza para aprobar la contraseña del BIOS.

Apagado y reinicio del sistema Windows de manera remota

Puede apagar o reiniciar el sistema Windows de manera remota mediante el uso del método RequestStateChange.

- 1 Apague el sistema Windows de manera remota utilizando el siguiente comando:

```
(gwmi -ComputerName "SYSNAME" -Namespace root\dcim\sysman DCIM_ComputerSystem | Where-Object {$_.Dedicated -ne 28}).RequestStateChange(3)
```

- 2 Reinicie el sistema Windows de manera remota utilizando el siguiente comando:

```
(gwmi -ComputerName "SYSNAME" -Namespace root\dcim\sysman DCIM_ComputerSystem | Where-Object {$_.Dedicated -ne 28}).RequestStateChange(11)
```

Obtención del valor de la hora del sistema Windows de manera remota

Puede obtener el valor de la hora del sistema Windows de manera remota con el método ManageTime. Por ejemplo:

En la interfaz de la línea de comandos, ejecute lo siguiente:

```
a $cred = Get-Credential
b $session = New-CimSession -ComputerName "Server01" -Credential $cred
c Get-CimInstance -CimSession $session -Namespace root\dcim\sysman -ClassName DCIM_TimeService | Invoke-CimMethod -MethodName ManageTime -Arguments @{GetRequest="TRUE"}
```

Administración local de sistemas cliente de Dell

Puede administrar los sistemas cliente de Dell de manera local usando los siguientes métodos:

- Para sistemas que ejecutan Windows, [mediante el uso de PowerShell](#).
- Para sistemas que ejecutan Linux, [mediante el uso de OMICLI](#).

Temas:

- [Administración local de sistemas Windows mediante PowerShell](#)
- [Administración local de sistemas Linux mediante OMICLI](#)

Administración local de sistemas Windows mediante PowerShell

Puede administrar sistemas cliente de Dell que ejecuten Windows localmente mediante el uso de comandos PowerShell.

- **Enumeración de instancias de una clase de DCIM**

- `Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSEnumeration`
- `Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSPassword`

- **Obtención de propiedades para una configuración del BIOS**

```
Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSEnumeration | Where-Object
{$_ .AttributeName -eq "Num Lock"}
```

- **Cambio de la configuración del BIOS**

```
Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSService | Invoke-CimMethod -
MethodName SetBIOSAttributes -Arguments @{AttributeName=@"Num Lock";AttributeValue=@"1"}
```

- **Modificación de valores no críticos**

```
Get-CimInstance -Namespace root\dcim\sysman DCIM_NumericSensor | Where-Object {$_ .DeviceID -
like "Root/MainSystemChassis/TemperatureObj:3"} | Set-CimInstance -Property
@{UpperThresholdNonCritical="10"}
```

- **Suscripción a alertas**

```
$a = 0
$timespan = New-Object System.TimeSpan(0, 0, 1)
$scope = New-Object System.Management.ManagementScope("\\.\root\dcim\sysman")
$query = New-Object System.Management.WQLEventQuery("Select * from DCIM_AlertIndication")
$watcher = New-Object System.Management.ManagementEventWatcher($scope,$query)
[array]$alerts=@()
do{ $watcher.WaitForNextEvent() }
while ($a -ne 1)
```

Administración local de sistemas Linux mediante OMICLI

Puede administrar los sistemas Linux de manera local mediante comandos de OMICLI. En los sistemas que ejecutan Linux, OMICLI se encuentra instalada en `/opt/omi/bin`.

- **Enumeración de instancias de una clase de DCIM**

- `./omicli ei root/dcim/sysman DCIM_BIOSEnumeration`

```
- ./omicli ei root/dcim/sysman DCIM_BIOSPassword
```

- **Obtención de propiedades para una configuración del BIOS**

```
./omicli gi root/dcim/sysman { DCIM_BIOSPassword InstanceID DCIM:BIOSSetupPassword }
```

- **Configuración de la contraseña de administrador**

```
./omicli iv root/dcim/sysman { DCIM_BIOSService Name DCIM:BiosService SystemCreationClassName  
DCIM_ComputerSystem SystemName <system name from DCIM_BIOSService class> CreationClassName  
DCIM_BIOSService } SetBIOSAttributes { AttributeName "AdminPwd" AttributeValue dell }
```

- **Cambio de la configuración del BIOS**

```
- ./omicli iv root/dcim/sysman { DCIM_BIOSService Name DCIM_BiosService  
SystemCreationClassName DCIM_ComputerSystem SystemName <system name in DCIM_BIOSService  
class> CreationClassName DCIM_BIOSService } SetBIOSAttributes { AttributeName "Num Lock"  
AttributeValue "1" AuthorizationToken "" }
```

```
- ./omicli iv root/dcim/sysman { DCIM_BIOSService Name DCIM:BiosService  
SystemCreationClassName DCIM_ComputerSystem SystemName <system name from DCIM_BIOSService  
class> CreationClassName DCIM_BIOSService } SetBIOSAttributes { AttributeName "AdminPwd"  
AttributeValue <password> }
```

```
./omicli iv root/dcim/sysman { DCIM_BIOSService Name DCIM:BiosService SystemCreationClassName  
DCIM_ComputerSystem SystemName <system name from DCIM_BIOSService class> CreationClassName  
DCIM_BIOSService } SetBIOSAttributes { AttributeName "AdminPwd" AttributeValue <password> }
```

- **Suscripción a alertas**

```
./omicli sub root/dcim/sysman --queryexpr "select * from DCIM_AlertIndication"
```

Administración remota de sistemas cliente de Dell

Puede administrar los sistemas cliente de Dell de manera remota usando cualquiera de los siguientes métodos:

- Para sistemas que ejecutan Windows, [Administración de un sistema Windows a través de un sistema Windows de manera remota mediante el uso de PowerShell](#)
- Para sistemas que ejecutan Linux, [Administración remota del sistema Linux a través del sistema de Windows mediante WinRM](#)

Temas:

- [Administración de un sistema Windows a través de un sistema Windows de manera remota mediante el uso de PowerShell](#)
- [Administración remota del sistema Linux a través del sistema de Windows mediante WinRM](#)
- [Administración remota de un sistema Linux a través de un sistema Linux mediante el uso de WSMAN](#)

Administración de un sistema Windows a través de un sistema Windows de manera remota mediante el uso de PowerShell

Puede acceder a un sistema Windows y supervisarlo de manera remota a través de un sistema de Windows mediante el uso de PowerShell.

Requisitos previos para el sistema Windows de administración:

- Windows PowerShell 3.0
- PowerShell configurado para ejecutar secuencias de comandos remotas

Requisitos previos para el sistema Windows administrado:

- Dell Command | Monitor
- Windows PowerShell 3.0
- PowerShell configurado para ejecutar secuencias de comandos remotas
- La función de comunicación remota de PowerShell debe estar activada

① NOTA:

Para utilizar Windows PowerShell de manera remota, la computadora remota debe estar configurada para la administración remota. Para obtener más información, incluidas las instrucciones, ejecute el comando de PowerShell `- Get-Help about_remote_requirements`.

Administración remota del sistema Linux a través del sistema de Windows mediante WinRM

Puede acceder al sistema que ejecuta Linux y supervisarlo a través del sistema que ejecuta Microsoft Windows mediante el uso de comandos de WinRM.

Requisitos previos para el sistema de Windows

- Sistema operativo Windows compatible
- Servicios de WinRM en funcionamiento y configurados para la administración remota

Requisitos previos para el sistema de Linux

- Privilegios de administrador
- Dell Command | Monitor
- Sistema operativo Linux compatible
- Activar los puertos 5985 y 5986 en el servidor WMI
- Sistema configurado para su entorno

En la interfaz de la línea de comandos, ejecute

```
winrm enumerate wsman/<DCM class name>?__cimnamespace=root/dcim/sysman -auth:basic -r:http://
<system IP or system name:5985> -username:<user name> -password:<password> -skipCAcheck -
skipCNcheck -encoding:utf-8
```

Administración remota de un sistema Linux a través de un sistema Linux mediante el uso de WSMAN

Puede acceder al sistema que ejecuta Linux y supervisarlos de forma remota a través del sistema que ejecuta Linux mediante el uso de comandos de WSMAN.

Requisitos previos para el sistema Linux de administración:

- Paquete de sistema operativo Linux compatible instalado
- Paquete wsmancli instalado

Requisitos previos para el sistema Linux administrado:

- Privilegios de acceso de administrador
- Sistema operativo Linux compatible
- Dell Command | Monitor

Inicie una terminal y ejecute

```
wsman enumerate http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/root/dcim/sysman/ <class
name> -N root/dcim/sysman -h <system ip/name> -u <user name> -p <password> -P 5985 -y
basic -v -V
```

Preguntas frecuentes

¿Cómo se encuentra el orden de inicio (secuencia) de la configuración de inicio con la propiedad `DCIM_OrderedComponent.AssignedSequence`?

Cuando una instancia `DCIM_BootConfigSetting` (heredada o UEFI) tiene varias instancias `DCIM_BootSourceSetting` (dispositivos de inicio) asociadas a través de instancias de la asociación `DCIM_OrderedComponent`, el valor de la propiedad `DCIM_OrderedComponent.AssignedSequence` se utiliza para determinar la secuencia en la que las instancias `DCIM_BootSourceSetting` asociadas (dispositivos de inicio) se utilizan durante el proceso de inicio. `DCIM_BootSourceSetting`, cuya propiedad `DCIM_OrderedComponent.AssignedSequence` asociada es igual a `0`, se ignora y no se considera parte del orden de inicio.

¿Cómo se cambia el orden de inicio?

El orden de inicio puede cambiarse con el método `DCIM_BootConfigSetting.ChangeBootOrder()`. El método `ChangeBootOrder()` establece el orden en el que se asocian las instancias `DCIM_BootSourceSetting` con una instancia `DCIM_BootConfigSetting`. El método tiene un parámetro de entrada; **Fuente**. El parámetro **Fuente** es un arreglo ordenado de la propiedad `PartComponent` de la clase `DCIM_OrderedComponent` que representa la asociación entre las instancias `DCIM_BootSourceSetting` (dispositivos de inicio) y la instancia `DCIM_BootConfigSetting` (tipo de lista de inicio heredada o UEFI).

¿Cómo se desactivan los dispositivos de inicio?

Al cambiar el orden de inicio, el valor de la propiedad `AssignedSequence` en cada instancia de `DCIM_OrderedComponent`, que asocia la instancia `DCIM_BootConfigSetting` de destino con la instancia `DCIM_BootSourceSetting` que no está presente en el arreglo de entrada del parámetro **Fuente**, se establece en `0`, lo que indica que el dispositivo se encuentra desactivado.

Al conectarse con el espacio de nombre con `wbemtest`, aparece un mensaje de inicio de sesión con error. ¿Cómo se resuelve este problema?

Inicie `wbemtest` con nivel de privilegio de administrador para resolver cualquier mensaje de inicio de sesión con error. Vaya a Internet Explorer en la lista **Todos los programas**, haga clic con el botón derecho del mouse y haga clic en **Ejecutar como administrador** para iniciar el `wbemtest` y evitar cualquier error relacionado con el espacio de nombre.

¿Cómo se ejecutan las secuencias de comandos de TechCenter sin que surjan problemas?

A continuación, se proporcionan los requisitos previos durante la ejecución de secuencias de comandos de VBS proporcionados en el vínculo de TechCenter de Dell Command | Monitor:

- 1 Configure **winrm** en el sistema con el comando `winrm quickconfig`.
- 2 Compruebe si el sistema es compatible con el token. Para ello, consulte:
 - La **Pantalla F2** en Configuración del BIOS.

- Utilice herramientas como **wbemtest** para comprobar si el valor de clave definido en la secuencia de comandos existe en el sistema.

① **NOTA:** Dell recomienda utilizar el BIOS más reciente disponible en dell.com/support. Para obtener más información, consulte la Guía de referencia de Dell Command | Monitor en dell.com/dellclientcommandssuitemanuals.

① **NOTA:** Utilice la versión del BIOS más reciente disponible.

¿Cómo se establecen los atributos del BIOS?

Es posible cambiar los atributos del BIOS con el método **DCIM_BIOSService.SetBIOSAttributes()**. El método **SetBIOSAttributes()** establece el valor de la instancia definida en la clase **DCIM_BIOSEnumeration**. El método tiene siete parámetros de entrada. Los primeros dos parámetros pueden estar vacíos o nulos. El tercer parámetro **AttributeName** debe utilizar la entrada que se asigna al valor de la instancia de nombre de atributo de la clase **DCIM_BIOSEnumeration**. El cuarto parámetro o **AttributeValue** puede ser cualquier valor posible de **AttributeName** según aparece definido en la clase **DCIM_BIOSEnumeration**. Si la contraseña del BIOS está establecida en el sistema, debe proporcionar esa misma contraseña en el quinto argumento. Los argumentos sexto y séptimo pueden estar vacíos o nulos.

¿Dell Command | Monitor admite la supervisión del almacenamiento y el sensor para sistemas operativos Windows y Linux?

Sí, Dell Command | Monitor admite tanto la supervisión del almacenamiento como la del sensor para sistemas operativos Windows y Linux compatibles.

En la supervisión de almacenamiento, Dell Command | Monitor admite la supervisión y las alertas de:

- La controladora integrada Intel (compatible con CSM v0.81 o posterior)
- las controladoras RAID integradas LSI; y 9217, 9271, 9341, 9361 y sus controladores asociados (físico y lógico)

① **NOTA:** La supervisión de la controladora integrada Intel no es compatible con los sistemas que ejecutan el sistema operativo Linux.

En la supervisión de sensores, Dell Command | Monitor admite la supervisión y las alertas del voltaje, la temperatura, el amperaje, los dispositivos de enfriamiento (ventilador) y los sensores de chasis.

Para obtener más información sobre la clase y las alertas, consulte la Guía de referencia de Dell Command | Monitor en dell.com/dellclientcommandssuitemanuals.

¿Puede Dell Command | Monitor estar integrado con otras aplicaciones o consolas?

Sí, Dell Command | Monitor interactúa con consolas de administración empresarial líderes que cumplen con los estándares de la industria. Se puede integrar con las siguientes herramientas de administración empresarial existentes:

- Dell Client Integration Suite para System Center 2012
- Dell OpenManage Essentials
- Dell Client Management Pack para System Center Operations Manager

¿Puedo importar clases en SCCM para el inventario?

Sí, los archivos OMCI_SMS_DEF.mof o MOF individuales se pueden importar en la consola SCCM para el inventario.

¿Dónde está ubicado el archivo SCCM OMCI_SMS_DEF.mof de la consola SCCM?

El archivo OMCI_SMS_DEF.mof está ubicado en C:\Program Files\Dell\Command_Monitor\ssa\omacim\OMCI_SMS_DEF.mof.

Solución de problemas

Temas:

- No se puede conectar de forma remota al Instrumental de administración de Windows
- Error de instalación en sistemas que ejecutan Windows
- El valor de enumeración de la configuración del BIOS aparece como 1
- No se puede instalar Hapi debido a la dependencia de libsmbios
- Recursos CIM no disponibles
- No se pueden ejecutar los comandos mediante DCM en los sistemas que ejecutan Ubuntu Core 16

No se puede conectar de forma remota al Instrumental de administración de Windows

Si la información del Modelo de información común (CIM) de un sistema informático cliente remoto no está disponible para la aplicación de administración o si falla una actualización remota del BIOS que utiliza el Modelo de objeto de componente distribuido (DCOM), aparecerán los siguientes mensajes de error:

- **Acceso denegado**
- **Win32: el servidor RPC no está disponible**

- 1 Compruebe que el sistema cliente esté conectado a la red. Para ello, en el símbolo de comando del servidor, escriba:
`ping <Host Name or IP Address>` y presione <Enter>.
- 2 Si tanto el servidor como el sistema cliente se encuentran en el mismo dominio, realice el siguiente paso:
 - Compruebe que la cuenta de administrador del dominio tenga privilegios de administrador para ambos sistemas.

Si el servidor y el sistema cliente se encuentran en un grupo de trabajo (pero no en el mismo dominio), realice el siguiente paso:

- Asegúrese de que el servidor se está ejecutando en la versión más reciente de Windows Server.

NOTA: Respalde los archivos de datos del sistema antes de realizar cambios en el registro. Si edita el registro de manera incorrecta, es probable que no pueda usar el sistema operativo.

- 3 Edite el cambio de registro en el sistema cliente. Haga clic en **Inicio > Ejecutar**, escriba **regedit** y, a continuación, haga clic en **Aceptar**. En la ventana **Editor de registro**, vaya a **My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa**.
- 4 Establezca el valor **forceguest** en **0** (el valor predeterminado es **1**). A menos que modifique este valor, el usuario que se conecta en forma remota al sistema tendrá privilegios de invitado, aunque las credenciales que proporcione tengan privilegios de Administrador.
 - a Cree una cuenta en el sistema cliente con el mismo nombre de usuario y contraseña, como si la cuenta de administrador del sistema ejecutara la aplicación de administración WMI.
 - b Si usa IT Assistant, ejecute la utilidad IT Assistant ConfigServices (**configservices.exe** en el directorio **/bin** bajo el directorio de instalación de IT Assistant). Configure IT Assistant para que se ejecute bajo una cuenta de administrador local, que también se conoce como administrador en el cliente remoto. También verifique que DCOM y CIM estén activados.
 - c Si usa IT Assistant, use la cuenta de administrador para configurar el descubrimiento de subred en el sistema del cliente. Introduzca el nombre de usuario como **<nombre de la máquina del cliente>\<nombre de la cuenta>**. Si el sistema ya se ha descubierto, elimínelo de la lista de sistemas descubiertos, configure el descubrimiento de subred para el mismo y vuelvo a descubrirlo.

NOTA: Dell recomienda utilizar Dell OpenManage Essentials como reemplazo de IT Assistant. Para obtener más información acerca de Dell OpenManage Essentials, consulte dell.com/dellclientcommandssuitemanuals.

NOTA: Utilice Dell OpenManage Essentials como reemplazo de IT Assistant.

- 5 Realice los pasos siguientes para modificar los niveles de privilegio de usuario a fin de conectarse de manera remota al WMI de un sistema.
 - a Haga clic en **Inicio > Ejecutar**, escriba `compmgmt.msc` y, a continuación, haga clic en **Aceptar**.
 - b Vaya a **Control de WMI** en **Servicios y aplicaciones**.
 - c Haga clic con el botón derecho del mouse en **Control de WMI** y, a continuación, haga clic en **Propiedades**.
 - d Haga clic en la pestaña **Seguridad** y seleccione **DCIM/SYSMAN** dentro del árbol **Raíz**.
 - e Haga clic en **Seguridad**.
 - f Seleccione el usuario o grupo específico cuyo acceso desee controlar y utilice la casilla **Permitir** o **Denegar** para configurar los permisos.
- 6 Realice los siguientes pasos para conectarse con un WMI (`root\DCIM\SYSMAN`) en un sistema desde un sistema remoto mediante WMI CIM Studio:
 - a Instale las **Herramientas de WMI** junto con `wbemtest` en el sistema local y, a continuación, instale Dell Command | Monitor en el sistema remoto.
 - b Configure el servidor de seguridad en el sistema para establecer una conexión remota con WMI. Por ejemplo, abra los puertos TCP 135 y 445 en el servidor de seguridad de Windows.
 - c Establezca el valor de **Seguridad local** como **Clásico: usuarios locales autenticados como ellos mismos para acceso de red: modelo de seguridad y uso compartido para cuentas locales** en la **Política de seguridad local**.
 - d Conéctese al WMI (`root\DCIM\SYSMAN`) en el sistema local desde un sistema remoto mediante WMI `wbemtest`. Por ejemplo, `\[Dirección IP del sistema remoto de destino]\root\DCIM\SYSMAN`
 - e Introduzca las credenciales de administrador del sistema remoto de destino si se las solicitan.

Para obtener más información acerca de WMI, consulte la documentación correspondiente de Microsoft en msdn.microsoft.com.

Error de instalación en sistemas que ejecutan Windows

Si no puede completar la instalación de Dell Command | Monitor para Windows, asegúrese de que:

- cuenta con privilegios de administrador en el sistema de destino.
- El sistema de destino sea un sistema fabricado por Dell con SMBIOS versión 2.3 o posterior.
- La consola de PowerShell no debe estar abierta.

NOTA: Para consultar la versión de SMBIOS del sistema, vaya a **Inicio > Ejecutar**, ejecute el archivo `msinfo32.exe` y compruebe la versión de SMBIOS en la página **Resumen del sistema**.

NOTA: El sistema debe ejecutar el sistema operativo Microsoft Windows compatible.

NOTA: El sistema tiene que actualizarse a .NET 4.0 o versiones posteriores.

El valor de enumeración de la configuración del BIOS aparece como 1

- 1 Verifique que se instalen los siguientes paquetes con privilegios de administrador:
 - `omi-1.0.8.ssl_100.x64.rpm`
 - `svradmin-hapi-8.3.0-1908.9058.el7.x86_64`
 - `command_monitor-linux-<número de versión>-<número BUID>.x86_64.rpm`
- 2 Si se instalan los paquetes anteriores, verifique que el módulo de controlador se encuentre cargado.
 - a Verifique que se cargue el módulo de controlador ejecutando el siguiente comando: `lsmod | grep dcdbas`.
 - b Si el módulo de controlador no se encuentra disponible, recupere los detalles del controlador ejecutando del siguiente comando `modinfo dcdbus`.
 - c Cargue el módulo de controlador ejecutando el siguiente comando: `insmod <filename>`.

No se puede instalar Hapi debido a la dependencia de libsmbios

Si no se puede realizar la instalación debido a problemas de dependencia:

Fuerce la instalación de todos los paquetes dependientes ejecutando `apt-get -f install`.

Recursos CIM no disponibles

Durante la enumeración, si recibe el error "Recurso CIM no disponible":

Verifique que los comandos se ejecuten con privilegios de administrador.

No se pueden ejecutar los comandos mediante DCM en los sistemas que ejecutan Ubuntu Core 16

Asegúrese de que la versión de la instantánea en el sistema sea 2.23 o posterior.

Otros documentos que puede necesitar

Además de esta Guía de usuario, puede acceder a los siguientes documentos en dell.com/dellclientcommandsuite/manuals. Haga clic en Dell Command | Monitor (anteriormente, OpenManage Client Instrumentation) y, a continuación, haga clic en el enlace de la versión correspondiente del producto en la sección **Asistencia general**.

Además de esta Guía de usuario, puede acceder a las siguientes guías.

- La *Guía de referencia de Dell Command | Monitor* proporciona información detallada acerca de todas las clases, propiedades y descripciones.
- La *Guía de instalación de Dell Command | Monitor* proporciona información sobre la instalación.
- La *Guía de referencia de SNMP de Dell Command | Monitor* proporciona la Base de información de administración (MIB) del Protocolo simple de administración de red (SNMP) correspondiente al Dell Command | Monitor.

Cómo ponerse en contacto con Dell

NOTA: Si no tiene una conexión a Internet activa, puede encontrar información de contacto en su factura de compra, en su albarán de entrega, en su recibo o en el catálogo de productos Dell.

Dell proporciona varias opciones de servicio y asistencia en línea y por teléfono. La disponibilidad varía según el país y el producto y es posible que algunos de los servicios no estén disponibles en su área. Si desea ponerse en contacto con Dell para tratar cuestiones relacionadas con las ventas, la asistencia técnica o el servicio de atención al cliente:

- 1 Vaya a **Dell.com/support**.
- 2 Seleccione la categoría de soporte.
- 3 Seleccione su país o región en la lista desplegable **Elija un país o región** que aparece al final de la página.
- 4 Seleccione el enlace de servicio o asistencia apropiado en función de sus necesidades.

Temas:

- [Otros documentos que puede necesitar](#)
- [Acceso a documentos desde el sitio de asistencia de Dell EMC](#)

Otros documentos que puede necesitar

Además de esta Guía de usuario, puede acceder a los siguientes documentos en **dell.com/dellclientcommandsuitemanuals**. Haga clic en Dell Command | Monitor (anteriormente, OpenManage Client Instrumentation) y, a continuación, haga clic en el enlace de la versión correspondiente del producto en la sección **Asistencia general**.

Además de esta Guía de usuario, puede acceder a las siguientes guías.

- La *Guía de referencia de Dell Command | Monitor* proporciona información detallada acerca de todas las clases, propiedades y descripciones.
- La *Guía de instalación de Dell Command | Monitor* proporciona información sobre la instalación.
- La *Guía de referencia de SNMP de Dell Command | Monitor* proporciona la Base de información de administración (MIB) del Protocolo simple de administración de red (SNMP) correspondiente al Dell Command | Monitor.

Acceso a documentos desde el sitio de asistencia de Dell EMC

Puede acceder a los documentos necesarios mediante una de las siguientes formas:

- Para ver documentos de EMC Connections Enterprise Systems Management: [Dell.com/SoftwareSecurityManuals](https://dell.com/SoftwareSecurityManuals)
- Para ver documentos de Dell EMC OpenManage: [Dell.com/OpenManageManuals](https://dell.com/OpenManageManuals)
- Para ver documentos de Dell EMC Remote Enterprise Systems Management: [Dell.com/esmmanuals](https://dell.com/esmmanuals)
- Para ver documentos de iDRAC y Dell EMC Lifecycle Controller: [Dell.com/idracmanuals](https://dell.com/idracmanuals)
- Para ver documentos de EMC OpenManage Connections Enterprise Systems Management: [Dell.com/OMConnectionsEnterpriseSystemsManagement](https://dell.com/OMConnectionsEnterpriseSystemsManagement)
- Para ver documentos de Dell EMC Serviceability Tools: [Dell.com/ServiceabilityTools](https://dell.com/ServiceabilityTools)
- a Vaya a [Dell.com/Support/Home](https://dell.com/Support/Home).
- b Haga clic en **Elegir entre todos los productos**.

- c En la sección **Todos los productos**, haga clic en **Software y seguridad** y, a continuación, haga clic en el vínculo necesario entre los siguientes:
 - **Administración de sistemas empresariales**
 - **Administración remota de sistemas empresariales**
 - **Herramientas de servicio**
 - **Conjunto de comandos del cliente de Dell**
 - **Administración de las conexiones de los sistemas del cliente**
- d Para ver un documento, haga clic en la versión del producto requerida.
- Mediante los motores de búsqueda:
 - Escriba el nombre y la versión del documento en el cuadro de búsqueda.