

Dell Command | Monitor Versión 9.0

Guía del usuario



Notas, precauciones y avisos

-  **NOTA:** Una NOTA proporciona información importante que le ayuda a utilizar mejor su equipo.
-  **PRECAUCIÓN:** Una PRECAUCIÓN indica la posibilidad de daños en el hardware o la pérdida de datos, y le explica cómo evitar el problema.
-  **AVISO:** Un mensaje de AVISO indica el riesgo de daños materiales, lesiones corporales o incluso la muerte.

Copyright © 2014 Dell Inc. Todos los derechos reservados. Este producto está protegido por leyes internacionales y de los Estados Unidos sobre los derechos de autor y la propiedad intelectual. Dell™ y el logotipo de Dell son marcas comerciales de Dell Inc. en los Estados Unidos y en otras jurisdicciones. El resto de marcas y nombres que se mencionan en este documento pueden ser marcas comerciales de las compañías respectivas.

2014 - 09

Rev. A00


Tabla de contenido

1 Introducción.....	5
Dell Command Monitor Descripción general.....	5
Arquitectura de Command Monitor	6
Novedades de esta versión	7
Características.....	7
Esquema de compatibilidad CIM 2.17.....	8
Configuración del BIOS.....	8
Seguridad de WMI.....	8
Informe de sucesos.....	8
Apagado remoto	8
Acceso a la información	8
Información de propiedad detallada	8
Configuración de encendido remoto	9
Modificación remota de la configuración del sistema.....	9
Estado y condición del sistema	9
Supervisión y alertas RAID para controladoras Intel y LSI.....	9
Supervisión y capturas SNMP.....	9
2 Estándares y protocolos	10
Descripción general de la tecnología de CIM, SNMP, WMI y WSMAN	10
CIM.....	10
SNMP.....	10
WMI.....	11
WSMAN.....	12
PowerShell	12
3 Requisitos del sistema	13
Requisito de hardware	13
Requisitos de software.....	13
4 Escenarios de usuarios	14
Escenario 1: administración de la propiedad	14
Integración con SCCM	14
Escenario 2: administración de la configuración.....	15
Escenario 3: supervisión de la condición.....	15
Supervisión de sucesos del sistema mediante indicación CIM o visor de sucesos de Windows	15
Escenario 4: Perfiles.....	16

Perfil de la batería	16
Perfil de administración del BIOS	16
Control de inicio	16
Base Desktop Mobile	17
Escritura en registro	17
Propiedad física	17
Perfil de memoria del sistema	17
5 Uso de Dell Command Monitor.....	18
Configuración del intervalo de sondeo	18
Creación de informes del estado RAID	18
Supervisión de los sistemas cliente	19
Detección de unidades de formato avanzado	19
Configuraciones de inicio	19
DCIM_BootConfigSetting.....	19
DCIM_BootSourceSetting.....	20
DCIM_OrderedComponent.....	20
Cambio de la secuencia de inicio mediante el método ChangeBootOrder.....	20
Configuración de atributos del BIOS	21
6 Preguntas frecuentes	22
¿Cómo se encuentra el orden de inicio (secuencia) de la configuración de inicio con la propiedad DCIM_OrderedComponent.AssignedSequence?.....	22
¿Cómo se cambia el orden de inicio?	22
¿Cómo se desactivan los dispositivos de inicio?.....	22
Al conectarse con el espacio de nombre con wbemtest, aparece un mensaje de inicio de sesión con error. ¿Cómo se resuelve este problema?.....	22
¿Cómo se ejecutan las secuencias de comandos de TechCenter sin que surjan problemas?	23
¿Cómo se establecen los atributos del BIOS?	23
7 Solución de problemas.....	24
No se puede conectar de forma remota al Instrumental de administración de Windows	24
Falla de instalación	25
8 Cómo ponerse en contacto con Dell.....	26
Otros documentos que podrían ser de utilidad.....	26
Acceso a documentos desde el sitio de asistencia de Dell.....	26

Introducción

Client Instrumentation representa las aplicaciones de software que permiten administrar de forma remota un sistema cliente. El software Dell Command | Monitor (Command | Monitor) activa la administración remota mediante el uso de programas de aplicaciones para acceder a la información del sistema cliente empresarial, supervisar el estado o cambiar el estado del sistema, como apagar el sistema de manera remota. Command | Monitor utiliza los parámetros clave del sistema a través de interfaces estándares, lo que les permite a los administradores administrar el inventario, supervisar la condición de los sistemas y recopilar información de los sistemas empresariales implementados. Este documento proporciona una descripción general de Dell Command | Monitor y sus funciones.

 **NOTA:** Dell Command | Monitor anteriormente se denominaba Dell OpenManage Client Instrumentation (OMCI). Después de OMCI versión 8.2.1, OMCI ahora se denomina Dell Command | Monitor.

Dell Command | Monitor Descripción general

Command | Monitor administra sistemas cliente mediante el modelo de información común (CIM) estándar y el protocolo simple de administración de red (SNMP), que son protocolos de administración. Esto reduce el costo total de propiedad, mejora la seguridad y ofrece un enfoque integral para administrar todos los dispositivos, incluso clientes, servidores y dispositivos de software, red y almacenamiento.


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

Command | Monitor contiene el conjunto de controladores subyacente que recopila información del sistema de distintas fuentes, lo que incluye el BIOS, CMOS, BIOS de System Management (SMBIOS), System Management Interface (SMI), el sistema operativo, la interfaz de programación de aplicaciones (API), la biblioteca de vínculos dinámicos (DLL) y valores de configuración del registro. Command | Monitor obtiene esta información a través de la interfaz del Administrador de objetos de CIM (CIMOM), la pila del Instrumental de administración de Windows (WMI) o el agente SNMP.

Command | Monitor les permite a los administradores de TI recopilar información de propiedad de manera remota, modificar la configuración de CMOS, recibir notificaciones proactivas sobre condiciones de error potenciales y obtener alertas de posibles infracciones de seguridad. Estas alertas están disponibles como sucesos en el registro de sucesos, indicación de CIM o se reciben como capturas SNMP después de importar el archivo de Base de información de administración (MIB) y supervisarlos.

Command | Monitor se usa para recopilar inventario de propiedad del sistema, incluso la configuración del BIOS, a través de la implementación de CIM o del agente de SNMP. 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 Command |

Monitor. Además, se pueden crear secuencias de comandos personalizadas para abordar áreas de interés clave. Puede usar estas secuencias de comandos para supervisión del inventario, configuración del BIOS y condición del sistema.

 **NOTA:** La instalación predeterminada no activa la compatibilidad con SNMP. Para obtener más información acerca de cómo activar la compatibilidad de SNMP, consulte la *Dell Command | Monitor Guía de instalación* en dell.com/clientsystemsmangement.

Arquitectura de Command | Monitor

El proveedor de datos de Command | Monitor recopila datos de información del sistema y almacena la información en formato de lenguaje de marcas extensible (XML) con propiedad exclusiva. El administrador de datos es un servicio que carga estos proveedores según la solicitud. La capa del proveedor CIM de Command | Monitor extrae la interfaz a distintas implementaciones de CIMOM. La entrada es una combinación de datos XML y lenguaje de hojas de datos extensible (XSL) en formato patentado, mientras que la salida es una instancia de objeto CIM basada en los perfiles de administración. El WSMAN que funciona como protocolo del canal solicita datos de CIMOM y los transmite a la consola.

La arquitectura de Command | Monitor cuenta con varias capas integradas con la pila del Instrumental de administración de Windows (WMI) de Microsoft:

- Capa de aplicaciones WMI: consta de aplicaciones de administración, herramientas de administración basadas en estándares y aplicaciones WMI como Microsoft SMS, LANDesk y herramientas WMI. Las aplicaciones de esta capa consumen los datos de administración del sistema proporcionados por Command | Monitor. Estas aplicaciones solicitan información de cliente y envían alertas a través de WSMAN y del administrador de objetos de CIM (CIMOM).
- Proveedor WMI CIM: se encuentra debajo de CIMOM y contiene dos proveedores CIM registrados en CIMOM:
 - El proveedor de instancias o métodos implementa una interfaz que permite realizar operaciones de utilidad como crear, eliminar, modificar y consultar.
 - El proveedor de indicaciones implementa una interfaz para las indicaciones (o sucesos) WMI. Cuando el CIMOM recibe una solicitud de información, la dirige al proveedor adecuado. Todos los proveedores están presentes en esta capa y proporcionan información sobre los dispositivos del sistema. Los proveedores envían solicitudes de aplicaciones de administración desde el CIMOM al enrutador de datos.
- Administrador de datos: carga el proveedor de datos según la solicitud de la capa superior.
- Proveedor de datos: recopila información del sistema como, por ejemplo, datos de hardware, controladores y sistema operativo, y los almacena en formato XML patentado.

La arquitectura de Command | Monitor cuenta con varias capas adicionales integradas con la pila SNMP:

- Agente SNMP: muestra los datos recibidos del administrador de datos, como tablas y capturas SNMP.
- MIB: los archivos MIB almacenan información acerca de tablas SNMP, sus atributos y las capturas disponibles.

Por ejemplo, una consola de administración de la capa de aplicaciones WMI le solicita al procesador disponible información sobre un sistema del cliente. La capa de aplicaciones WMI le envía la solicitud a través de la red al CIMOM del sistema del cliente. El CIMOM le pasa la solicitud al proveedor y administrador de datos de Command | Monitor. El administrador de datos carga el proveedor de datos correspondiente, que obtiene la información y la almacena en un formato patentado. Luego la

información regresa a la consola de administración (a través de la misma ruta de acceso en sentido inverso).

Novedades de esta versión

- El nombre actual de Dell OpenManage Client Instrumentation (OMCI) es Dell Command | Monitor
- Compatibilidad para supervisión y alertas para arreglo redundante de LSI de controladora de discos independientes (RAID)
- Compatibilidad para supervisión y alertas de todas las sondas del sensor
- No se admiten los espacios de nombre (**root/dellomci**) heredados
- Compatibilidad para SNMP 10909 MIB nuevo
- Compatibilidad con los testigos nuevos siguientes:
 - GPS Radio
 - Retroiluminación del teclado con CA
 - Cámara trasera
 - Bloqueo <Fn>
 - Modo de bloqueo <Fn>
 - Tarjeta de interfaz de red (NIC) no administrada integrada
 - Unmanaged NIC
 - Rear USB Ports (Puertos USB traseros)
 - Side USB Ports (Puertos USB laterales)
 - Trusted Execution
- Compatibilidad para valores adicionales, **medium_high** y **medium_low** para el testigo **fanspeed**.



NOTA: Se han eliminado los espacios de nombre heredados y SNMP 10892 MIB.

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

Características

Las funciones clave de Command | Monitor son:

- Esquema de compatibilidad CIM 2.17
- Configuración del BIOS
- Seguridad de WMI
- Informe de sucesos
- Apagado remoto
- Acceso a la información del sistema mediante el protocolo WMI-CIM, WSMAN y SNMP
- 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 Intel y LSI.
- Supervisión y capturas SNMP

Esquema de compatibilidad CIM 2.17

Command | Monitor respeta 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

Configuración del BIOS

Command | Monitor ofrece la capacidad de configurar el BIOS del sistema, incluida la administración del orden de inicio.

Seguridad de WMI

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.

La seguridad de WMI puede configurarse con WMI Control, disponible en la consola de administración del equipo en la sección Servicios y aplicaciones. Haga clic con el botón derecho del mouse en **WMI Control** y, a continuación, haga clic en **Propiedades**. Puede configurar la seguridad específica del espacio de nombre desde la ficha **Seguridad**. **WMI Control** También puede ejecutarse desde el menú **Inicio** o desde la **CLI** al ejecutar `wmimgmt.msc`.

Informe de sucesos

Command | Monitor detecta los sucesos en los sistemas Dell y envía alertas al usuario local y al administrador de red sobre errores potenciales, cambios en la configuración e intrusiones en el chasis. Una aplicación de administración de sistemas, tal como Open Manage Essentials (OME), muestra estos sucesos.

Apagado remoto

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

Acceso a la información

Command | Monitor proporciona acceso a la información del sistema como revisión del BIOS y modelo del sistema a través de WMI con CIM. También se puede usar el protocolo WSMAN para acceder a esta información a través de WMI.

Información de propiedad detallada

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

Configuración de encendido remoto

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

Modificación remota de la configuración del sistema

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

Estado y condición del sistema

Command | Monitor supervisa la condición del sistema, como el estado del ventilador, e informa sobre su estado a través de anotaciones de registro de sucesos NT y sucesos CIM.

Supervisión y alertas RAID para controladoras Intel y LSI.

Supervisión y alertas para las unidades físicas y lógicas de las controladoras Intel y LSI.

Supervisión y capturas SNMP

Command | Monitor es compatible con SNMP v1 y admite la supervisión de los atributos y las capturas del sistema.

Estándares y protocolos

Command | Monitor utiliza el Instrumental de administración de Windows (WMI) de Microsoft y activa los protocolos de Web Services-Management (WSMAN). Command | Monitor utiliza el protocolo simple de administración de red (SNMP) para describir diversas variables del sistema.

Descripción general de la tecnología de CIM, SNMP, WMI y WSMAN

El grupo Desktop Management Task Force (DMTF, Grupo de tareas de administración de escritorio) 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.

CIM

El Modelo de información común (CIM), creado por DMTF como parte de la iniciativa de Administración de empresas basadas en web (WBEM), ofrece una vista unificada de los objetos físicos y lógicos en el entorno administrado.

A continuación, se muestran detalles importantes del CIM:

- CIM es un modelo de datos orientado a objetos para describir información de administración. CIM describe la manera en la que se organizan los datos, no necesariamente el modelo de transporte usado para transportarlos. El método de transporte más común es WMI.
- Las aplicaciones de administración admitidas para CIM recopilan información de una variedad de dispositivos y objetos de CIM, incluidos sistemas cliente y servidor, dispositivos de infraestructura de red y aplicaciones.
- El estándar CIM proporciona detalles sobre técnicas de asignación que ofrecen una mejor compatibilidad con otros protocolos de administración.
- El modelo de datos CIM extrae y describe todos los elementos de un entorno de red. El esquema CIM proporciona las descripciones del modelo de datos real y organiza la red en una serie de objetos administrados interrelacionados y clasificados ampliamente.
- El esquema CIM se define mediante el archivo de Formato de objeto administrado (MOF), que proporciona un modelo estandarizado para describir la información de administración entre clientes en un sistema de administración. El archivo MOF no se limita a una implementación en particular y permite intercambiar información de administración entre distintos sistemas de administración y clientes.

SNMP

SNMP (protocolo simple de administración de red) es una solución ampliamente aceptada para administrar dispositivos en redes de protocolo de Internet (IP). El grupo Internet Engineering Task Force (IETF, Grupo de trabajo de ingeniería de Internet) desarrolla y mantiene el protocolo SNMP. Command |

Monitor accede a información y supervisa sistemas cliente mediante SNMP. Los dispositivos que generalmente admiten SNMP son enrutadores, conmutadores, servidores, estaciones de trabajo, la mayoría de los componentes de hardware, entre otros. Consiste en un conjunto de normas para la administración de la red, incluidos un protocolo de capa de aplicaciones, un esquema de base de datos y un conjunto de objetos de datos. SNMP presenta los datos de administración en forma de variables en los sistemas administrados, que describen la configuración del sistema. Las aplicaciones de administración pueden consultar estas variables.

SNMP no define la información (las variables) que un sistema administrado debe ofrecer. En cambio, SNMP utiliza un diseño extensible, donde la lista de la información disponible la definen las bases de información de administración (MIB). Las MIB describen la estructura de los datos de administración de un dispositivo y sus subsistemas. Las MIB utilizan un espacio de nombre jerárquico que contiene identificadores de objeto (OID). Cada OID identifica una variable que puede ser leída mediante SNMP.

WMI

WMI es la implementación dedicada de Microsoft de Web-based Enterprise Management (WBEM). Se implementa en las plataformas Microsoft Windows. WMI admite extensiones CIM y extensiones CIM específicas de Microsoft.

WMI incluye:

- Un conjunto de servicios nativos eficaz, tal como la recuperación de información basada en consultas y la notificación de eventos.
- Capacidades extensas de secuencias de comandos a través del host de secuencias de comandos de Windows (WSH).
- El CIMOM, que es una interfaz y un punto de manipulación de los objetos y la información CIM.
- El repositorio, donde CIMOM almacena los datos de administración.

En la arquitectura de Command | Monitor, CIMOM y el repositorio se representan a través del Administrador de objetos de WMI de Microsoft. CIMOM es la interfaz y el punto de manipulación para información u objetos de CIM. Actúa como un facilitador de la recopilación de información y manipulación de las propiedades de los objetos. Microsoft ha implementado este componente como el servicio de administración de Windows (winmgmt). CIMOM es una capa intermedia de software que media las interacciones entre las aplicaciones de administración de nivel superior y la instrumentación de niveles inferiores, como Command | Monitor y otros proveedores. CIMOM garantiza que los datos proporcionados por los proveedores se presenten a las aplicaciones de administración de manera uniforme e independiente del proveedor. CIMOM hace esto a través de la interfaz de programación de aplicaciones (API) del modelo de objetos componentes (COM).

El repositorio es un archivo binario donde CIMOM almacena los datos de administración. Los datos incluyen información de archivos de formato de objeto administrado (MOF) compilados, incluso definiciones de clases, propiedades, calificadores y relaciones jerárquicas de CIM. Los datos de la instancia se almacenan aquí a medida que se encuentran disponibles.

WMI proporciona una interfaz de secuencias de comandos. Mediante VBScript o JScript, se pueden escribir secuencias de comandos, establecer conexión con los servicios WMI de forma local o remota, recuperar información o ejecutar métodos. Es posible crear secuencias de comandos para la mayoría de las tareas de Command | Monitor ya que este último se implementa a través de WMI.

Para obtener más información acerca de VBScript y las secuencias de comandos de ejemplo, consulte la *Guía de referencia de Dell Command | Monitor* disponible en dell.com/clientsystemsmangement.

Para obtener más información acerca de WMI, consulte technet.microsoft.com.



NOTA: Para realizar una conexión remota a servicios WMI, debe tener privilegios de administrador en ambos sistemas, el local y el remoto.

WSMAN

El protocolo WSMAN es un estándar DMTF abierto que define un protocolo basado en el protocolo simple de acceso a objetos (SOAP) para administrar servidores, dispositivos, aplicaciones y servicios web. Usa datos de CIMOM para facilitar la administración.

WSMAN es un protocolo que proporciona una capa de abstracción para acceder a la información de CIM. La razón es que la consola puede usar WSMAN para comunicarse con sistemas en banda o fuera de banda para recopilar inventario de propiedad y para establecer información o ejecutar métodos. En los sistemas en banda, la capa de WSMAN también extrae el sistema operativo que se encuentra debajo. Sin embargo, Command | Monitor no requiere WSMAN y no activa directamente WSMAN ya que se trata de un protocolo solamente.

Para obtener más información acerca de la administración de WSMAN desde DMTF, consulte dmtf.org/standards/wsman.

Para obtener más información acerca de la activación de la administración basada en WS de WMI en un sistema que ejecuta el sistema operativo Windows, consulte msdn.microsoft.com/en-us/library/aa384426%28v=VS.85%29.aspx.

Para obtener más información acerca de los perfiles de DMTF que se utilizan en Command | Monitor, consulte la *Guía de referencia de Dell Command | Monitor* en dell.com/clientsystemsmangement.

PowerShell

Windows PowerShell es un entorno de administración de configuración y automatización de tareas de Microsoft. PowerShell consta de un shell de línea de comando y lenguaje de línea de comandos asociado incorporado a .NET Framework. PowerShell proporciona acceso completo a WMI y COM, lo que les permite a los administradores realizar las tareas administrativas como la configuración y la supervisión de sistemas locales y remotos que ejecutan un sistema operativo Windows mediante los servicios de Command | Monitor.

Los administradores pueden escribir secuencias de comandos de PowerShell personalizadas (archivos con sufijo **.ps1**) que se conectan al espacio de nombre de DCIM y permiten supervisar las acciones personalizadas en el sistema.

Requisitos del sistema

Este capítulo proporciona información acerca de los requisitos de hardware y software de Command | Monitor.

Requisito de hardware

Requisito	Detalles
System (Sistema)	Sistema de cliente Enterprise con SMBIOS 2.3 o posterior.

Requisitos de software

Requisito	Detalles
Sistema operativo compatible	<ul style="list-style-type: none">• Microsoft Windows 8.1• Microsoft Windows 8• Microsoft Windows 7• Microsoft Windows Vista
Marco admitido	<ul style="list-style-type: none">• Microsoft .NET 4.0

Escenarios de usuarios

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

Puede utilizar Command | Monitor para:

- Administración de la propiedad
- Administración de la configuración
- Supervisión de la condición
- Perfiles

Escenario 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 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 Command | Monitor en cada sistema Dell, el administrador de TI puede recopilar información de forma rápida y 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 determinar los sistemas que se pueden actualizar a las versiones más recientes de Windows.

También es posible obtener el inventario de propiedad a través de una secuencia de comandos o cualquier línea de comandos del Instrumental de administración de Windows (WMI).

Integración con SCCM

Es posible integrar SCCM con Command | Monitor mediante:

- El uso del archivo MOF incluido en el paquete de instalación de Command | Monitor, que contiene todas las clases de 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.

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

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

La configuración estandarizada proporciona un ahorro de costos significativo a 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 del equipo. Con 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 activar Wake On LAN (WOL) para que el sistema pueda volver a encenderse a partir de un estado inactivo durante las horas no pico para realizar tareas de administración de sistemas.

Escenario 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 parece que ahora puede acceder a los archivos. El usuario ignora el problema inicial porque parece que se ha solucionado solo. Mientras tanto, Command | Monitor le consulta el problema al disco duro para buscar alguna falla predictiva y envía una alerta de Tecnología de autosupervisión, análisis e informes (SMART) a la consola de administración. También le muestra el error SMART al usuario local. La alerta indica que están ocurriendo varios errores de lectura o escritura en el disco duro. El departamento de TI de la empresa le recomienda al usuario hacer una copia de seguridad de los archivos de datos críticos inmediatamente. Se envía a un técnico de servicio con una unidad de reemplazo.

Se reemplaza el 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 sucesos del sistema mediante indicación CIM o visor de sucesos de Windows

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

- Transmisión del registro a través de la clase WMI **DCIM_LogEntry**.
- Supervisión de la indicación CIM a través de la clase **DCIM_AlertIndication**.
- Supervisión de sucesos mediante el protocolo simple de administración de red (SNMP).

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

Escenario 4: Perfiles

Los administradores de TI deben controlar el sistema cliente en entornos empresariales distribuidos y de múltiples proveedores. Se enfrentan con numerosos desafíos ya que deben dominar diversos conjuntos 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 Command | Monitor. Algunos de los perfiles de DMTF se explican en esta guía.

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

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 el valor del atributo del BIOS se puede 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 administració (AdminPwd). Ejecute el método **DCIM_BIOSService.SetBIOSAttributes()** y establezca AdminPwd en AttributeName y el valor de contraseña en los parámetro 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 anotaciones de registro individuales. Obtenga todas las instancias de **DCIM_LogEntry** asociadas con la instancia determinada de **DCIM_RecordLog** a través de la asociación **DCIM_LogManagesRecord**. Clasifique las instancias según **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 las escrituras en registro según la marca de hora de la anotación del registro. Obtenga todas las instancias de **DCIM_LogEntry** asociadas con la instancia determinada de **DCIM_RecordLog** a través de la asociación **DCIM_LogManagesRecord**. Clasifique las instancias **DCIM_LogEntry** según el valor de la propiedad **CreationTimeStamp** en el orden último en entrar, primero en salir (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

Para ver la información que proporciona Command | Monitor, acceda a:

- `root\dcim\sysman (standard)`


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

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

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 los archivos `dcsbdy32.ini` o `dcsbdy64.ini`. El archivo `dcsbdy32/64.ini` se encuentra en la siguiente ubicación:

`<Command | Monitor installed location>\omsa\ini`

 **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

Command | Monitor activa 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. Las versiones 9.0 y posteriores de Command | Monitor también admiten controladoras LSI para la función de supervisión y alertas.

Supervisión de los sistemas cliente

Command | Monitor admite el protocolo simple de administración de red (SNMP) para supervisar y administrar sistemas cliente tales como equipos portátiles, escritorios y estaciones de trabajo. El archivo de base de información de administración (MIB) se comparte entre Command | Monitor y Server Administrator.

Se ha modificado Command | Monitor 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 acerca de SNMP, consulte la *Dell Command | Monitor Guía de referencia de SNMP* en dell.com/clientsystemsmanagement.

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. Command | Monitor le permite identificar 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

Un sistema cliente puede tener dos configuraciones 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 para representar, 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 los dispositivos de inicio o las fuentes. Las propiedades **ElementName**, **BIOSBootString** y **StructuredBootString** contienen una cadena que identifica los dispositivos de inicio. Por ejemplo, disco flexible, disco duro, CD/DVD, red, Personal Computer Memory Card International Association (PCMCIA), Battery Electric Vehicle (BEV) o USB. Según el tipo de lista de inicio del dispositivo, se asocia la instancia de **DCIM_BootSourceSetting** 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 secuencia de inicio mediante el método ChangeBootOrder

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

1. Busque el tipo de lista de inicio mediante:
 - Comando 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. Busque el tipo de orden de inicio (heredada o UEFI) mediante:
 - Comando 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. Cambie el orden de inicio mediante:
 - Comando WMIC: `wmic /namespace:\\root\dcim\sysman path dcim_bootconfigsetting call ChangeBootOrder /?:full`
 - Comando PowerShell: `(gwmi -namespace root\dcim\sysman -class dcim_bootconfigsetting).getmethodparameters("ChangeBootOrder")`

Los argumentos necesarios para el método **ChangeBootOrder** son:

- Señal de autorización: esta es la contraseña de inicio o de Administrador.

- Fuente: 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**.


Configuración de atributos del BIOS

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

- **SetBIOSAttributes:** para cambiar la configuración del BIOS
- **ChangeBootOrder:** para cambiar la configuración de inicio
- **RequestStateChange** - Para apagar y reiniciar el sistema
- **ManageTime:** devuelve la hora del sistema.

Puede ejecutar estos métodos con winrm, secuencias de comandos VB, comandos Powershell, wmic, wbenmtest.exe y WMI wbenmtest.

Puede establecer los atributos del BIOS con el método SetBIOSAttributes. El procedimiento se explica a continuación al activar el módulo de plataforma de confianza (TPM) a modo de ejemplo.

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

Para activar TPM:

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

```
(gwmi -Class DCIM_BIOSService -Namespace root\dcim
\sysman).SetBIOSAttributes($null,$null,"AdminPwd","enter a new password")
```

2. Para activar la seguridad de TPM, utilice el siguiente comando y reinicie el sistema después de que:

```
(gwmi -Class DCIM_BIOSService -Namespace root\dcim
\sysman).SetBIOSAttributes($null,$null,"Trusted Platform
Module","1","provide the password")
```

3. Para activar el TPM, utilice el siguiente comando y, nuevamente, reinicie el sistema:

```
(gwmi -Class DCIM_BIOSService -Namespace root\dcim
\sysman).SetBIOSAttributes($null,$null,"Trusted Platform Module
Activation","2","provide the password")
```

4. Reinicie el sistema.

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

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 al ejecutar secuencias de comandos de VBS proporcionados en el vínculo Techcenter de Command | Monitor:

1. Configure **winrm** en el sistema con el comando `winrm quickconfig`.
2. Verifique si el sistema es compatible con el testigo. Para ello, consulte:
 - La **Pantalla F2** en Configuración del BIOS.
 - Utilice herramientas como **wbemtest** para verificar si el valor de clave definido en la secuencia de comandos existe en el sistema.

 **NOTA:** Dell recomienda utilizar el BIOS más reciente disponible en dell.com/support.

¿Cómo se establecen los atributos del BIOS?

Es posible cambiar los atributos del BIOS con el método **DCIM_BootService.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.

Solución de problemas

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. Verifique 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:
 - Verifique 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: Haga una copia de seguridad de los archivos de datos de su sistema antes de realizar cambios en el registro. Si edita el registro en forma 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/clientsystemsmanagement.


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 ficha **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 pasos siguientes 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.

Falla de instalación

If you are unable to complete Dell Command | Monitor installation, ensure that:


- You have Administrator privileges on the target system.
- The target system is a Dell manufactured system with SMBIOS version 2.3 or later.

 **NOTA:** To check the SMBIOS version on the system, go to **Start** → **Run** and run the `msinfo32.exe` file and check for the SMBIOS version in System Summary page.

 **NOTA:** The system must be running supported Microsoft Windows operating system.

 **NOTA:** The system has to be upgraded to .NET 4.0 or later versions.

Cómo ponerse en contacto con Dell

 **NOTA:** Si no dispone de una conexión a Internet activa, puede encontrar información de contacto en la factura de compra, en el albarán o en el catálogo de productos de Dell.

Dell proporciona varias opciones de servicio y asistencia en línea o telefónica. Puesto que la disponibilidad varía en función del país y del producto, es posible que no pueda disponer de algunos servicios 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.

Otros documentos que podrían ser de utilidad

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

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

Acceso a documentos desde el sitio de asistencia de Dell

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

- Mediante los siguientes enlaces:
 - Para todos los documentos de Enterprise Systems Management: **dell.com/softwaresecuritymanuals**
 - Para documentos de Enterprise System Management: **dell.com/openmanagemanuals**
 - Para documentos de Remote Enterprise System Management: **dell.com/esmanuals**
 - Para documentos de OpenManage Connections Enterprise Systems Management: **dell.com/OMConnectionsEnterpriseSystemsManagement**
 - Para documentos de Herramientas de servicio: **dell.com/serviceabilitytools**

- Para documentos de Client Systems Management: **dell.com/clientsystemsmanagement**
- Para documentos de OpenManage Connections Client Systems Management: **dell.com/connectionsclientsystemsmanagement**
- En el sitio web de asistencia de Dell:
 - a. Vaya a **dell.com/support/home**.
 - b. En la sección **Asistencia general**, haga clic en **Software y seguridad**.
 - c. En el grupo **Software y seguridad**, haga clic en el vínculo requerido que corresponda:
 - **Administración de sistemas Enterprise**
 - **Administración remota de sistemas Enterprise**
 - **Herramientas de servicio**
 - **Administración de sistemas cliente**
 - **Administración de conexiones de sistemas 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 buscar.