

Dell Command | Monitor Versión 10.6

Guía del usuario



Notas, precauciones y advertencias

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

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

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

Tabla de contenido

Capítulo 1: Introducción a Dell Command Monitor 10.6.....	5
Novedades de esta versión de Dell Command Monitor 10.6.....	5
Dell Command Monitor Visión general.....	5
Capítulo 2: Cumplimiento de la Tabla de mitigaciones de seguridad de Windows SMM (WSMT).....	7
Capítulo 3: Estándares y protocolos de Dell Command Monitor 10.6.....	8
Capítulo 4: Escenarios de casos de uso con Dell Command Monitor 10.6.....	9
Situación 1: Administración de recursos.....	9
Integración SCCM.....	9
Situación 2: Administración de la configuración.....	9
Situación 3: Monitoreo de la condición.....	10
Monitoreo de alertas del sistema mediante el visor de eventos, syslog o la indicación CIM del sistema operativo.....	10
Situación 4: Perfiles.....	10
Perfil de activo.....	10
Perfil de la batería.....	11
Perfil de administración del BIOS.....	11
Control de inicio.....	11
Base Desktop Mobile.....	12
Escritura en registro.....	12
Propiedad física.....	12
Perfil de memoria del sistema.....	12
Capítulo 5: Uso de Dell Command Monitor 10.6.....	13
Configuración del intervalo de sondeo.....	13
Creación de informes del estado RAID.....	13
Monitoreo de los sistemas cliente Dell.....	13
Registro de aplicaciones para Dell Command Monitor for Linux.....	14
Detección de unidades de formato avanzado.....	14
Configuraciones de inicio.....	14
DCIM_AssetWarrantyInformation.....	15
DCIM_BootConfigSetting.....	15
DCIM_BootSourceSetting.....	15
DCIM_OrderedComponent.....	16
Atributo DCIM_Smart.....	16
DCIM_ThermalInformation.....	16
Cambio de la configuración del sistema.....	16
Restablecimiento del BIOS a los valores predeterminados para sistemas con Windows o Linux.....	16
Configuración de atributos del BIOS en un sistema que ejecuta Windows mediante el uso de comandos PowerShell.....	18
Configuración de los atributos del BIOS en el sistema que ejecuta Linux.....	19
Cambio de la secuencia de inicio.....	21

Apagado y reinicio del sistema Windows de manera remota.....	22
Obtención del valor de la hora del sistema Windows de manera remota.....	22
Capítulo 6: Administración local de sistemas cliente de Dell mediante Dell Command Monitor 10.6.....	23
Administración local de sistemas Windows mediante PowerShell.....	23
Administración local de sistemas Linux mediante OMICLI.....	24
Capítulo 7: Administración remota de sistemas cliente Dell mediante Dell Command Monitor 10.6.....	25
Administración de un sistema Windows a través de un sistema Windows de manera remota mediante el uso de PowerShell.....	25
Administración remota del sistema Linux a través del sistema de Windows mediante WinRM.....	25
Administración remota de un sistema Linux a través de un sistema Linux mediante el uso de WSMAN.....	26
Capítulo 8: Preguntas más frecuentes para Dell Command Monitor 10.6.....	27
Capítulo 9: Pasos para la solución de problemas mediante Dell Command Monitor 10.6.....	29
No se puede conectar de forma remota al Instrumental de administración de Windows.....	29
Error de instalación en sistemas que ejecutan Windows.....	30
El valor de enumeración de la configuración del BIOS aparece como 1.....	30
No se puede instalar Hapi debido a la dependencia de libsmbios.....	30
Recursos CIM no disponibles.....	31
No se pueden ejecutar los comandos mediante DCM en los sistemas que ejecutan Ubuntu Core 16.....	31
Capítulo 10: Otros documentos que podrían ser de utilidad.....	32
Acceso a documentos desde el sitio de soporte de Dell.....	32
Capítulo 11: Cómo ponerse en contacto con Dell.....	33

Introducción a Dell Command | Monitor 10.6

La aplicación de software Dell Command | Monitor permite a los administradores de TI administrar fácilmente el inventario de la flota, supervisar el estado del sistema, modificar la configuración del BIOS y recolectar información de forma remota para los sistemas cliente Dell implementados.

El monitoreo del estado del sistema activo puede ayudar a reducir el costo total de propiedad del sistema y forma parte de un enfoque integral para administrar todos los dispositivos en red.

Dell Command | Monitor está diseñado para los sistemas cliente de Dell Enterprise y los sistemas Dell de puertas de enlace de IoT, así como para los equipos integrados de Dell.

En este documento, se presenta una visión general de Dell Command | Monitor y sus funciones. Para obtener más información acerca de los sistemas Dell compatibles, consulte las notas de la versión disponibles en dell.com/support.

Temas:

- [Novedades de esta versión de Dell Command | Monitor 10.6](#)
- [Dell Command | Monitor Visión general](#)

Novedades de esta versión de Dell Command | Monitor 10.6

- Compatibilidad con los siguientes atributos nuevos de BIOS:
 - Intel® GNA Accelerator
 - Multiple Atom Cores
 - USB4 CM Mode
 - Onboard Unmanaged NIC
 - Enable Pre-Boot DMA Support
 - Enable OS Kernel DMA Support
 - PCIe Resizable Base Address Register (BAR)
 - OS Agent Requests
 - Enable Microsoft UEFI CA
 - Legacy Manageability Interface Access
 - Power-on-Self-Test (POST) Automatic Recovery
- Soporte para el método **ResetBIOSDefaults**.

Dell Command | Monitor Visión general

 **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 Simple Network Management Protocol (SNMP), los cuales son protocolos de administración. Esto ayuda a reducir el costo total de propiedad del sistema, mejora la seguridad y proporciona un enfoque completo para administrar todos los dispositivos dentro de un dispositivo de red.

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 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 recolecta información del sistema del cliente a partir de la biblioteca de vínculos dinámicos (DLL) y la configuración del registro. Dell Command | Monitor para Windows recupera esta información a través de la interfaz del Administrador de objetos CIM.

(CIMOM), la pila del Instrumental de administración de Windows (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 Dell Command | Monitor les permite a los administradores de TI recopilar información de propiedad de manera remota, modificar la configuración de BIOS, recibir notificaciones proactivas sobre condiciones de error potenciales y obtener alertas de posibles infracciones 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 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 Knowledge Library 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. Si desea obtener más información acerca de cómo activar la compatibilidad de SNMP de Dell Command | Monitor para Windows, consulte la guía de instalación de Dell Command | Monitor en dell.com/support.

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 indica el cambio de comportamiento debido al cumplimiento de 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.

 **NOTA:** Para obtener más información sobre las plataformas soportadas, consulte [Plataformas soportadas](#).

Estándares y protocolos de Dell Command | Monitor 10.6

Dell Command | Monitor se basa en 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 el monitoreo remoto.

 **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.

Escenarios de casos de uso con Dell Command | Monitor 10.6

En esta sección, se describen varias situaciones de casos de uso de Dell Command | Monitor.

Puede utilizar Dell Command | Monitor para lo siguiente:

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

Temas:

- Situación 1: Administración de recursos
- Situación 2: Administración de la configuración
- Situación 3: Monitoreo de la condición
- Situación 4: Perfiles

Situación 1: Administración de recursos

Una empresa que usa muchos sistemas Dell no pudo mantener la precisión en su información de inventario debido a cambios en el negocio y el personal de TI. El gerente de informática (CIO) solicita un plan para identificar los sistemas que pueden actualizarse a la versión más reciente de Windows. Para ello, se deben evaluar los sistemas implementados para 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 interrupciones al usuario final.

Mediante Dell 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 identificar los sistemas que se pueden actualizar a la versión más reciente 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

Puede integrar SCCM en Dell Command | Monitor mediante:

- El uso del archivo MOF incluido en el paquete de instalación de Dell Command | Monitor, el cual 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, 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 cada computadora cliente sin visitar manualmente cada 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 arranque. OpenManage Essentials (OME) es una consola de administración que se puede integrar en Dell Command | Monitor y utilizar para supervisar la configuración del BIOS de manera remota en todos los sistemas cliente. 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 sobre Dell Command | Monitor, consulte la guía de referencia de Dell Command | Monitor en **dell.com/support**.

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 activar la tecnología Wake On LAN (WOL) para reactivar el sistema desde un estado inactivo durante las horas de baja actividad a fin de realizar tareas de administración de sistemas.

Situación 3: Monitoreo 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.

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

Dell Command | Monitor admite el monitoreo de sucesos 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) Monitoreo 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) Monitoreo mediante syslog.

Para obtener más información sobre Dell Command | Monitor, consulte la guía de referencia de Dell Command | Monitor en **dell.com/support**.

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 en Dell Command | Monitor los perfiles estándar del sector del Grupo de trabajo de administración distribuida (DMTF) y de Administración de infraestructura de centros de datos (DCIM-OEM). Algunos de los perfiles de DMTF se explican en esta guía.

Para obtener más información sobre Dell Command | Monitor, consulte la guía de referencia de Dell Command | Monitor en **dell.com/support**.

Perfil de activo

Estado de la garantía en el dispositivo terminal:

- Para determinar el estado de la garantía, enumere u obtenga la instancia de la clase **DCIM_AssetWarrantyInformation**.
- Compruebe si el estado de la garantía se puede determinar mediante las propiedades **WarrantyStartDate** y **WarrantyEndDate** de la clase **DCIM_AssetWarrantyInformation**.

NOTA: El requisito previo para **DCIM_AssetWarrantyInformation** es que debe contar con una conexión a Internet activa. Si está ejecutando Dell Command | Monitor detrás de un servidor proxy, asegúrese de que la configuración del proxy esté establecida correctamente.

Para obtener más información sobre el estado de la garantía de los periféricos, haga lo siguiente:

1. Vaya a Dell.com/support.
 2. Seleccione su país o región en la lista desplegable Elija un país o región que aparece al final de la página
 3. Seleccione la categoría de soporte: garantía y contratos
 4. Proporcione la etiqueta de servicio apropiada de su sistema
- Deshabilite la función de garantía y las llamadas posteriores de actualización.
 - Extraiga la información de garantía a pedido.
- NOTA:** La información de la garantía se actualiza automáticamente cada 15 días. En caso de un estado de garantía reciente, la información de la garantía indicada podría no ser la misma que aparece en el sitio de soporte de Dell.

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 estado 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**.
- Determine la ubicación de la batería y el ePPID de esta mediante las propiedades **IdentifyingDescriptions** y **OtherIdentifyingInfo** de la clase **DCIM_Battery**.

DCIM_Battery

Para obtener la información sobre el valor del ePPID de la batería para un elemento de esta. Abra un símbolo del sistema de PowerShell con privilegio de administrador y ejecute el siguiente comando `Get-CimInstance -Namespace root/dcim/sysman -Classname DCIM_Battery |Select ElementName, OtherIdentifyingInfo, IdentifyingDescriptions`.

NOTA: El valor del ePPID de la batería no es dinámico y si se reemplaza esta última, debe reiniciar el sistema para reflejar los cambios en la instancia de **DCIM_Battery**.

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 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**.
- Puede utilizar el método **DCIM_ComputerSystem.RequestStateChange()** para establecer el valor del parámetro RequestedState en **3**. El valor del parámetro 3 apaga el sistema.
- Puede utilizar el método **DCIM_ComputerSystem.RequestStateChange()** para establecer el valor del parámetro **RequestedState** en **11**. El valor del parámetro 11 reinicia el sistema.
- 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 10.6

Para ver la información que proporciona Dell Command | Monitor, acceda a la siguiente ruta: `root\dcim\sysman (standard)`

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

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

Temas:

- [Configuración del intervalo de sondeo](#)
- [Creación de informes del estado RAID](#)
- [Monitoreo de los sistemas cliente Dell](#)
- [Registro de aplicaciones para Dell Command | Monitor for 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.

- En Windows, los archivos `dcsbdy32.ini` o `dcsbdy64.ini` se encuentran en `<Dell Command | Monitor installed location>\omsa\ini`.
- En Linux, el archivo `AlertPollingSettings.ini` se encuentra en `/opt/dell/dcm/conf`.

NOTA: Los números del archivo INI se multiplican por **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, lo que equivale a aproximadamente 3 horas).

Creación de informes del estado RAID

Dell Command | Monitor Dell Command | Monitor activa la información de la configuración de RAID y monitorea 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 el monitoreo 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.

Monitoreo de los sistemas cliente Dell

- Dell Command | Monitor Dell Command | Monitor para Windows admite el Simple Network Management Protocol (SNMP) para el monitoreo y la administración de sistemas cliente tales como laptops, equipos de escritorio y estaciones de trabajo. El archivo de la Base de datos de información de administración (MIB) se comparte entre Dell Command | Monitor y Server Administrator. Dell Command | MonitorSe modificó Dell 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 sobre SNMP, consulte la guía de referencia de SNMP de Dell Command | Monitor en dell.com/support.

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

Registro de aplicaciones para Dell Command | Monitor for 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 se pueden ver 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:

 **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.

 **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.

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

- BackupIndex: el usuario puede especificar el conteo de sustitución del archivo **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 el disco duro de un sistema es una unidad de AF de 4 KB, lo cual 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 arranque (heredado o UEFI) se modela con las siguientes clases:

- DCIM_ElementSettingData
- DCIM_BootConfigSetting
- DCIM_OrderedComponent
- DCIM_BootSourceSetting
- DCIM_SmartAttributeInfo

NOTA: Los términos Configuración de inicio y Tipo de lista de inicio se utilizan indistintamente y transmiten el mismo significado, sea que representen la configuración heredada o UEFI.

DCIM_AssetWarrantyInformation

- Para consultar el estado de la garantía en el dispositivo terminal, ejecute el siguiente comando en el símbolo del sistema de PowerShell:

```
Get-CimInstance -Namespace root/DCIM/SYSMAN -ClassName DCIM_AssetWarrantyInformation
```

- Para ver los derechos de garantía de WarrantyEndDate en orden cronológico, ejecute el siguiente comando en el símbolo del sistema de PowerShell:

```
Get-CimInstance -Namespace root/dcim/sysman -ClassName DCIM_AssetWarrantyInformation |  
Sort-Object -Property WarrantyEndDate | Select Name, WarrantyEndDate, WarrantyStartDate
```

- Para desactivar la función de garantía y las llamadas posteriores de actualización, ejecute el siguiente comando en el símbolo del sistema de PowerShell:

```
Get-CimInstance -Namespace root/DCIM/SYSMAN -ClassName DCIM_AssetWarrantyInformation |  
Where-Object{$_ .InstanceID -eq "Root/MainSystemChassis/COOObject/COOWarranty:0"} | Invoke-  
CimMethod -MethodName DisableWarranty
```

- Para extraer la información de garantía según demanda, ejecute el siguiente comando en el símbolo del sistema de PowerShell:

```
Get-CimInstance -Namespace root/DCIM/SYSMAN -ClassName DCIM_AssetWarrantyInformation |  
Where-Object{$_ .InstanceID -eq "Root/MainSystemChassis/COOObject/COOWarranty:0"} | Invoke-  
CimMethod -MethodName RefreshWarranty
```

NOTA: Configurar para configuración de proxy:

- Proxy predeterminado: Dell Command | Monitor selecciona el proxy del sistema predeterminado (establecido en IE)
- Proxy personalizado

La clase **DCIM_ApplicationProxySetting** se utiliza con el fin de modificar la configuración de proxy para Dell Command | Monitoree según el ambiente proxy.

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 arranque: heredado 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, Personal Computer Memory Card International Association (PCMCIA), 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**.

Atributo DCIM_Smart

Para leer el valor del atributo smart, ejecute los siguientes comandos:

Por ejemplo:

- `Get-CimInstance -Namespace root\dcim\sysman DCIM_SmartAttributeInfo | Format-Table`
- `Get-CimInstance -Namespace root\dcim\sysman DCIM_SmartAttributeInfo -Filter "AttributeID like '< Attribute ID Value >'"`

Para configurar los valores de umbral personalizados, ejecute los siguientes comandos:

Por ejemplo:

- `Get-CimInstance -Namespace root\dcim\sysman DCIM_SmartAttributeInfo -Filter "AttributeID like '<Attribute ID Value>'" | Invoke-CimMethod -MethodName "SetCustomThreshold" -Arguments @{CustomThresholdValue="<custom threshold value to be set>"}`

DCIM_ThermalInformation

DCIM_ThermalInformation administra los ajustes de configuración térmica, como Modo térmico, Modo AAC y Modo de fallo del ventilador.

- Para consultar la información térmica del dispositivo, ejecute el siguiente comando:

```
Get-CimInstance -Namespace root/DCIM/SYSMAN -ClassName DCIM_ThermalInformation
```

- Para establecer el valor del modo térmico, ejecute el siguiente comando:

```
Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_ThermalInformation | Where-Object {$_.AttributeName -eq "Thermal Mode"} | Invoke-CimMethod -MethodName ChangeThermalMode -Arguments @{AttributeName=@"Thermal Mode";AttributeValue=@"2"}
```

Cambio de la configuración del sistema

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

- SetBIOSAttributes: cambia la configuración del BIOS
 **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.

Restablecimiento del BIOS a los valores predeterminados para sistemas con Windows o Linux

ResetBIOSDefaults (método)

Comando de PowerShell (WMI): `Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSService | Invoke-CimMethod -MethodName ResetBIOSDefaults -Arguments @{ DefaultType=<one of the possible values>}`

Comando de OMI: /omicli iv root/dcim/sysman { DCIM_BIOSService Name DCIM:BiosService SystemCreationClassName DCIM_ComputerSystem SystemName <ServiceTag> CreationClassName DCIM_BIOSService } ResetBIOSDefaults { DefaultType <one of the possible values> }

Los valores posibles son los siguientes:

- 0: Valores predeterminados seguros incorporados: esto se conoce como los valores predeterminados del BIOS. Esta configuración soporta cualquier plataforma y, por lo tanto, no se puede cambiar la configuración.
- 1: Último estado válido conocido: el BIOS genera esto de manera automática después de completar correctamente la POST. Esta opción revierte el BIOS a una configuración correcta. Si los **valores predeterminados seguros incorporados** están dañados, puede utilizar **Último estado válido conocido** para restaurar el BIOS.
- 2: Valores predeterminados de fábrica: los valores predeterminados de fábrica se generan antes de enviar el sistema. Esta configuración está optimizada para los ajustes de hardware o se personaliza según sus requisitos durante la compra o el servicio.
- 3: Configuración de usuario 1: se configura cuando el usuario lo requiere. Debe **guardar la configuración actual** en la configuración del BIOS o en la pantalla F2 para restablecer la configuración a través de la aplicación Dell Command | Monitor.
- 4: Configuración de usuario 2: se configura cuando el usuario lo requiere. Debe **guardar la configuración actual** en la configuración del BIOS o en la pantalla F2 para restablecer la configuración a través de la aplicación Dell Command | Monitor.

Tabla 1. Valores posibles de ResetBIOSDefaults

Descripción	Código de error (valor de SetResult)
Ejecución satisfactoria	0
Valor de entrada no válido/valor de entrada fuera del rango	1
Error de autenticación	2
Configuración no soportada	3
Configuración vacía	4
Falla genérica/no se realizó correctamente/cuando el servicio no está en ejecución	4294967295

NOTA: Es necesario reiniciar el sistema después de la operación **ResetBIOSDefaults** para que los cambios se apliquen correctamente.

Las ventanas de DCM tienen la funcionalidad de apagar o reiniciar el sistema a través de las siguientes API:

- Reiniciar el sistema: Get-CimInstance -Namespace ROOT\DCIM\SYSMAN -ClassName DCIM_ComputerSystem | Where-Object {\$_.Dedicated -ne 28} | Invoke-CimMethod -MethodName RequestStateChange -Arguments @{RequestedState='11'}
- Apagar el sistema: Get-CimInstance -Namespace ROOT\DCIM\SYSMAN -ClassName DCIM_ComputerSystem | Where-Object {\$_.Dedicated -ne 28} | Invoke-CimMethod -MethodName RequestStateChange -Arguments @{RequestedState='3'}

Las siguientes API se pueden utilizar en el sistema operativo GNU o Linux:

- shutdown -r +5
- sudo reboot

NOTA: Durante la operación de restablecimiento, un subconjunto de opciones no se restablece a los valores predeterminados. Esto puede ser por motivos de seguridad (por ejemplo, contraseñas) o capacidad de arranque (por ejemplo, lista de arranque y ROM de opciones heredadas).

Los registros de eventos del BIOS no se restablecen para almacenar el historial del hardware del sistema.

En la siguiente tabla, se enumera la lista completa de características que no se restablecen a los valores predeterminados.

Tabla 2. Lista completa de características que no se restablecen a los valores predeterminados

Sección	Subsección	Elemento
General	System Information	Etiqueta de servicio
	System Information	Asset Tag
	System Information	Ownership Tag
	Boot Sequence	Lista de arranque

Tabla 2. Lista completa de características que no se restablecen a los valores predeterminados (continuación)

Sección	Subsección	Elemento
	Advanced Boot Options	Activar OROM heredadas
	Fecha/Hora	Fecha/Hora
	Integrated NIC	Integrated NIC
	Integrated NIC	Enable UEFI Network Stack
	SATA Operation	SATA Operation
Security (Seguridad)	NA	Admin Password
	NA	System Password
	NA	Contraseñas de HDD-x interno
	NA	Bloqueo de contraseña maestra
	Mitigación de riesgos de SMM	Mitigación de riesgos de SMM
	Intel SGX Enable	Intel SGX Enable
Inicio seguro	Secure Boot Enable	Secure Boot Enable
	Expert Key Management	Bases de datos de claves

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.

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

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 -MethodName 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
-MMethodName 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
-MMethodName SetBIOSAttributes -Arguments @{AttributeName=@"Trusted Platform Module
Activation";AttributeValue=@"2";AuthorizationToken="<Admin password>"}
```

5. Reinicie el sistema.

Exención genérica de responsabilidad

El módulo Powershell PSReadline guarda cada comando de la consola que escribe en un archivo de texto. Así que le recomendamos que utilice el comandlet "Get-Credential" para manejar la contraseña de forma segura.

- a. \$cred = Get-Credential
- b. Escriba el nombre de usuario y la contraseña, por ejemplo, AdminPWD y Dell_123\$, cuando aparezca el cuadro de diálogo.
- c. \$BSTR = [System.Runtime.InteropServices.Marshal]::SecureStringToBSTR(\$cred.Password)

- d. \$plainpwd=[System.Runtime.InteropServices.Marshal]::PtrToStringAuto(\$BSTR)
- e. Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSService | Invoke-CimMethod MethodName SetBIOSAttributes -Arguments @{AttributeName=@"AdminPwd";AttributeValue=@" \$plainpwd"}}

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.

NOTA: Asegúrese de que la opción TPM esté 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=<system name from DCIM_BIOSService class>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.

NOTA: Asegúrese de que la opción TPM esté 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: `Get-WmiObject -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: `Get-WmiObject -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: `(Get-WmiObject -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:
`$boLegacy = Get-WmiObject -namespace root\\dcim\\sysman -class dcim_orderedcomponent | where {$_.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 = Get-WmiObject -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: `$boUefi = Get-WmiObject -namespace root\dcim\sysman -class dcim_orderedcomponent | where {$_.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 = Get-WmiObject -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 mediante Dell Command | Monitor 10.6

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)
```

- Comandos para obtener el consentimiento del usuario desde WMI:

```
Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_ImprovementProgramConsent
```

- Comandos para establecer el consentimiento del usuario desde WMI:

```
Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_ImprovementProgramConsent |
Invoke-CimMethod -MethodName OverrideImprovementProgramConsent -Arguments @{NewValue="1"}
```

NOTA: El programa de mejora está disponible para Dell Command | Monitor 10.5 y 10.6 de 64 bits.

- Comandos para obtener el proxy desde WMI:

```
Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_ApplicationProxySetting
```

- Comandos para establecer el proxy desde WMI:

```
Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_ApplicationProxySetting |
Invoke-CimMethod -MethodName ChangeProxySetting -Arguments @{NewAddress="10.0.0.223"; NewPort="8080"}
```

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 Dell mediante Dell Command | Monitor 10.6

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](#) en la página 25
- Para sistemas que ejecutan Linux, [Administración remota del sistema Linux a través del sistema de Windows mediante WinRM](#) en la página 25

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

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 Windows mediante comandos 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 el siguiente comando:

```
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 supervisarlo 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 más frecuentes para Dell Command | Monitor 10.6

- ¿Cómo puedo encontrar el orden (la secuencia) de arranque de la configuración de arranque 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 **CIM_OrderedComponent.AssignedSequence** asociada es igual a **0**, se ignora y no se considera parte del orden de inicio.

- ¿Cómo cambio el orden de arranque?

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_Ordered Component** 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 desactivo los dispositivos de arranque?

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.

- Se muestra un mensaje de inicio de sesión fallido cuando <lo que intenta conectar> intenta conectarse al espacio de nombres con `wbemtest`.

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 secundario. Luego, haga clic en **Ejecutar como administrador** para iniciar el **wbemtest** y evitar un error de espacio de nombre.

- ¿Cómo se ejecutan las secuencias de comandos de Knowledge Library sin que surjan problemas?

A continuación, se proporcionan los pasos para ejecutar los scripts VBS proporcionados en el enlace de la biblioteca de conocimientos 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 los valores clave definidos en el script existen en el sistema.

 **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/support.

- ¿Cómo establezco 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 asignada 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**. El quinto parámetro **AuthorizationToken** es opcional, la entrada del quinto parámetro es la contraseña del BIOS. El quinto parámetro se usa solamente cuando la contraseña del BIOS está establecida en el sistema, de lo contrario, está vacío. Los argumentos sexto y séptimo pueden estar vacíos o nulos.

- ¿Dell Command | Monitor soporta el monitoreo del almacenamiento y el sensor para sistemas operativos Windows y Linux?

Sí, Dell Command | Monitor soporta el monitoreo tanto del almacenamiento como del sensor para sistemas operativos Windows y Linux compatibles.

En el monitoreo de almacenamiento, Dell Command | Monitor admite el monitoreo y las alertas de:

- o La controladora integrada Intel (compatible con CSMI v0.81 o posterior)
 - o Las controladoras RAID integradas LSI; y 9217, 9271, 9341, 9361 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 el monitoreo de sensores, Dell Command | Monitor admite el monitoreo y las alertas del voltaje, la temperatura, el amperaje, los dispositivos de enfriamiento (ventilador) y los sensores del chasis.

Para obtener más información sobre clases y alertas, consulte la guía de referencia de Dell Command | Monitor en dell.com/support.

- ¿Dell Command | Monitor puede estar integrado en otras aplicaciones/consolas?

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

- o Dell Client Integration Suite para System Center 2012
- o Dell OpenManage Essentials
- o 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.

- ¿Cómo configurar el proxy para DCM 10.2.1?

- DCM 10.2.1 no puede obtener información sobre la garantía.

- Compruebe si la configuración del proxy de la aplicación está configurada correctamente mediante la clase DCIM_ApplicationProxySetting.

Cómo puedo configurar una credencial de proxy para Dell Command | Monitor.

Si inició sesión a través de Dell Command | Monitor, puede usar las mismas credenciales para la autenticación de proxy.

- Dell Command | Monitor no muestra la información de la garantía.

- o El sistema cliente no está conectado a Internet durante el sondeo.

Conéctese a Internet y extraiga la información de garantía mediante la ejecución del siguiente comando:

```
Get-CimInstance -Namespace root/DCIM/SYSMAN -ClassName DCIM_AssetWarrantyInformation |  
Where-Object{$_.InstanceID -eq "Root/MainSystemChassis/COOObject/COOWarranty:0"} | Invoke-  
CimMethod -MethodName RefreshWarranty
```

- o El sistema cliente no está configurado con el servidor proxy.

Configure los ajustes de proxy en Dell Command | Monitor mediante la ejecución de los siguientes comandos:

- Para obtener el proxy de WMI, ejecute el siguiente comando `Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_ApplicationProxySetting`.
- Para establecer el proxy de WMI, ejecute el siguiente comando `Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_ApplicationProxySetting | Invoke-CimMethod -MethodName Change ProxySetting -Arguments @{NewAddress="10.0.0.223"; NewPort="8080"}`

Debe reemplazar **NewAddress** y **NewPort** según el entorno del proxy (si corresponde).

Pasos para la solución de problemas mediante Dell Command | Monitor 10.6

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 **forcequest** 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 una cuenta de administrador en el 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. Ingrese 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/support.
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 wbmtest 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 wbmtest. 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 de Microsoft correspondiente en msdn.microsoft.com.

Error de instalación en sistemas que ejecutan Windows

Si no puede completar la instalación de Dell Command | Monitor, 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 un sistema operativo 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`
 - `srvadmin-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 dcdbas`.
 - 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 podrían ser de utilidad

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

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

- En la guía de referencia de Dell Command | Monitor, se proporciona información detallada acerca de todas las clases, propiedades y descripciones.
- En la guía de instalación de Dell Command | Monitor, se proporciona información sobre la instalación.
- En la guía de referencia de SNMP de Dell Command | Monitor, se proporciona la Base de datos de información de administración (MIB) del protocolo Simple Network Management Protocol (SNMP) correspondiente a Dell Command | Monitor.

Temas:

- [Acceso a documentos desde el sitio de soporte de Dell](#)

Acceso a documentos desde el sitio de soporte de Dell

También puede acceder a los documentos requeridos seleccionando su producto.

1. Vaya a www.dell.com/manuals.
2. Haga clic en **Examinar todos los productos**, haga clic en **Software** y, luego, haga clic en **Administración de sistemas cliente**.
3. Para ver los documentos necesarios, haga clic en el nombre del producto requerido y su número de versión.

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, el soporte técnico o el servicio al cliente, realice lo siguiente:

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.