

# Dell Command | Monitor versione 10.0

Guida dell'utente



## Messaggi di N.B., Attenzione e Avvertenza

 **N.B.:** un messaggio N.B. (Nota Bene) indica informazioni importanti che contribuiscono a migliorare l'utilizzo del prodotto.

 **ATTENZIONE:** Un messaggio di ATTENZIONE indica un danno potenziale all'hardware o la perdita di dati, e spiega come evitare il problema.

 **AVVERTENZA:** Un messaggio di AVVERTENZA indica un rischio di danni materiali, lesioni personali o morte.

© 2008 -2018 Dell Inc. o sue affiliate. Tutti i diritti riservati. Dell, EMC e gli altri marchi sono marchi commerciali di Dell Inc. o delle sue sussidiarie. Gli altri marchi possono essere marchi dei rispettivi proprietari.

<b>1 Introduzione.....</b>	<b>6</b>
Novità in questa versione.....	6
Panoramica di Dell Command   Monitor.....	6
<b>2 Conformità WSMT (Windows SMM Security Mitigations).....</b>	<b>8</b>
<b>3 Caratteristiche.....</b>	<b>9</b>
Supporto dello schema CIM.....	9
Configurazione ed enumerazione delle impostazioni del BIOS.....	9
Sicurezza WMI/OMI.....	9
Segnalazione di avvisi.....	10
Arresto remoto.....	10
Accesso alle informazioni di sistema.....	10
Informazioni dettagliate sulle risorse.....	10
Configurazione di attivazione remota.....	10
Modifica da remoto delle impostazioni del BIOS del sistema.....	10
Integrità e stato del sistema.....	10
Monitoraggio e generazione di avvisi di RAID per controller Intel e LSI.....	10
Monitoraggio e trap per SNMP.....	11
<b>4 Standard e protocolli.....</b>	<b>12</b>
<b>5 Scenari utente.....</b>	<b>13</b>
Scenario 1: gestione delle risorse.....	13
Integrazione di SCCM .....	13
Scenario 2: gestione della configurazione.....	14
Scenario 3: monitoraggio dell'integrità.....	14
Avvisi del sistema di monitoraggio mediante Visualizzatore eventi, Syslog, o indicazioni CIM del sistema operativo.....	14
Scenario 4: profili.....	15
Profilo batteria.....	15
Profilo di gestione del BIOS.....	15
Controllo dell'avvio.....	15
Base Desktop Mobile.....	15
Record del registro.....	16
Risorsa fisica.....	16
Profilo di memoria di sistema.....	16
<b>6 Utilizzo di Dell Command   Monitor.....</b>	<b>17</b>
Impostazione dell'intervallo di polling.....	17
Creazione di rapporti sullo stato del RAID.....	17
Monitoraggio dei sistemi client Dell.....	17
Registro applicazioni di Dell Command   Monitor per Linux.....	18

File di configurazione.....	18
Rilevamento delle unità del formato avanzato.....	18
Configurazioni di avvio.....	18
DCIM_BootConfigSetting.....	19
DCIM_BootSourceSetting.....	19
DCIM_OrderedComponent.....	19
Modifica delle impostazioni audio.....	19
Impostazione degli attributi del BIOS in un sistema Windows che utilizza i comandi PowerShell.....	20
Impostazione degli attributi del BIOS nel sistema Linux.....	20
Modifica dell'ordine di avvio.....	22
Arresto e riavvio del sistema operativo Windows da remoto.....	23
Come ottenere il valore dell'intervallo di tempo da remoto su un sistema Windows.....	23
<b>7 Gestione dei sistemi client Dell a livello locale.....</b>	<b>25</b>
Gestione locale dei sistemi Windows tramite PowerShell.....	25
Gestione locale dei sistemi Linux tramite OMICLI.....	25
<b>8 Gestione remota dei sistemi client di Dell.....</b>	<b>27</b>
Gestione da remoto del sistema Windows tramite Windows PowerShell.....	27
Gestione remota del sistema Linux tramite un sistema Windows che utilizza WinRM.....	27
Gestione remota del sistema Linux tramite un sistema Linux che utilizza WSMAN.....	28
<b>9 Domande frequenti.....</b>	<b>29</b>
Come si trova l'ordine di avvio (sequenza) della configurazione di avvio utilizzando la proprietà DCIM_OrderedComponent.AssignedSequence?.....	29
Come si modifica l'ordine di avvio?.....	29
Come si disabilitano i dispositivi di avvio?.....	29
Quando ci si collega allo spazio dei nomi con wbemtest, viene visualizzato un messaggio di accesso non riuscito. Com'è possibile risolvere il problema?.....	29
Come posso eseguire gli script di TechCenter senza alcun problema?.....	29
Come si impostano gli attributi del BIOS?.....	30
Dell Command   Monitor supporta il monitoraggio di storage e sensori per i sistemi operativi Windows e Linux?.....	30
È possibile integrare Dell Command   Monitor con altre applicazioni/console?.....	30
È possibile importare le classi in SCCM per l'inventario?.....	30
Dove si trova il file SCCM OMCI_SMS_DEF.mof?.....	30
<b>10 Risoluzione dei problemi.....</b>	<b>32</b>
Impossibile eseguire la connessione remota a Strumentazione gestione Windows.....	32
Errore di installazione sui sistemi che eseguono Windows.....	33
Il valore di enumerazione delle impostazioni del BIOS è 1.....	33
Errore di installazione HAPI dovuto a dipendenze da libsmbios.....	34
Le risorse CIM non sono disponibili.....	34
Impossibile eseguire i comandi utilizzando DCM sui sistemi che eseguono Ubuntu Core 16.....	34
<b>11 Altri documenti che potrebbero essere necessari.....</b>	<b>35</b>
<b>12 Come contattare Dell.....</b>	<b>36</b>

Altri documenti che potrebbero essere necessari.....	36
Accesso ai documenti dal sito di supporto Dell EMC.....	36

# Introduzione

L'applicazione software Dell Command | Monitor abilita la gestione remota usando programmi applicativi per accedere alle informazioni, monitorare lo stato oppure modificare lo stato del sistema come per esempio arrestare il sistema in remoto. Dell Command | Monitor usa parametri di sistema chiave tramite interfacce standard che consentono agli amministratori di gestire l'inventario, monitorare l'integrità del sistema e raccogliere informazioni sui sistemi Dell distribuiti. Dell Command | Monitor è progettato per sistemi client Dell Enterprise, sistemi Dell IoT Gateway, come anche per PC Dell Embedded. Per maggiori informazioni sui sistemi Dell supportati, fare riferimento alle note sulla versione disponibili all'indirizzo [dell.com/dellclientcommandsuitemanuals](https://dell.com/dellclientcommandsuitemanuals). Questo documento fornisce una panoramica di Dell Command | Monitor e delle sue funzioni.

**❗ N.B.: Dell Command | Monitor era precedentemente Dell OpenManage Client Instrumentation (OMCI). Dopo la versione 8.2.1 di OMCI, è stato ridenominato come Dell Command | Monitor.**

Argomenti:

- [Novità in questa versione](#)
- [Panoramica di Dell Command | Monitor](#)

## Novità in questa versione

Supporto per la conformità WSMT. Per ulteriori informazioni sulla conformità WSMT, consultare la sezione Conformità WSMT (Windows SMM Security Mitigations) nella Guida dell'utente di Dell Command | Monitor.

Supporto per le seguenti funzioni del BIOS:

- Auto Switch, Battery Slice Charge Configuration, BIOS Enumeration Mode, Broadcom TruManage, Dust Filter Maintenance, eMMC, Enable Block SID, Enable Tablet Button LED Sign of Life, Fan Speed Auto Level on Cpu Zone, Fan Speed Auto Level on Psu Zone, GraphicSpecMode, HDD0 Fan Enable, HDD4 Fan Enable, Intel Speed Shift Technology, PCIE0, PCIE1, PCIE0\_CPU1, PCIE1\_CPU1, PPI Bypass for Block SID Command, PPI Bypass for TPM Clear, Report Logo Type, SATA-8, Secure Boot Mode, SMM Security Mitigation, Slice Battery Custom Charge Limit e Wake on 2nd LAN (RJ-45/SFP).

Per ulteriori informazioni sugli attributi del BIOS, consultare la *Dell Command | Monitor Reference Guide* (Guida di riferimento di Dell Command | Monitor) all'indirizzo [dell.com/dellclientcommandsuitemanuals](https://dell.com/dellclientcommandsuitemanuals).

## Panoramica di Dell Command | Monitor

**❗ N.B.: Il protocollo SNMP (Simple Network Management Protocol) non è supportato in Dell Command | Monitor per Linux.**

Dell Command | Monitor gestisce i sistemi client utilizzando lo standard Common Information Model (CIM) e il protocollo SNMP (Simple Network Management Protocol), entrambi protocolli di gestione. Ciò consente di ridurre il costo totale di proprietà e di migliorare la sicurezza, fornendo un approccio olistico alla gestione tutti i dispositivi collegati a una rete, tra cui client, server, storage, sistemi di rete e dispositivi software.

Utilizzando CIM, è possibile accedere a Dell Command | Monitor tramite servizi WSMAN (Web Services for Management Standards).

Dell Command | Monitor contiene la serie fondamentale del driver che raccoglie le informazioni del sistema client da fonti differenti, tra cui il BIOS, CMOS, il BIOS della gestione del sistema (SMBIOS), System Management Interface (SMI), il sistema operativo, Interfaccia di programmazione delle applicazioni (API), Dynamic-Link Library (DLL) e le impostazioni del registro. Inoltre, Dell Command | Monitor per Windows raccoglie le informazioni sul sistema client dalle DLL (Dynamic-Link Library) e dalle impostazioni del registro. Dell Command | Monitor per Windows recupera queste informazioni dall'interfaccia CIM Object Manager (CIMOM), dallo stack di Strumentazione gestione

Windows (WMI) o dall'agente SNMP, mentre Dell Command | Monitor per Linux le recupera dall'interfaccia di Open Management Infrastructure (OMI).

Dell Command | Monitor consente agli amministratori di IT di raccogliere informazioni sugli asset da remoto, di modificare le impostazioni del BIOS e di ricevere notifiche proattive sulle potenziali condizioni di errore e avvisi sulle potenziali violazioni della sicurezza. Nei sistemi che eseguono Windows, questi avvisi sono disponibili nel registro eventi di NT, come eventi WMI o come trap SNMP v1. Per i sistemi Linux, questi avvisi vengono ricevuti come eventi SysLog, OMI o del registro applicazioni.

Dell Command | Monitor per Windows può essere integrato in una console come Microsoft System Center Configuration Manager, accedendo direttamente alle informazioni del CIM o tramite i fornitori di altre console che hanno implementato l'integrazione di Dell Command | Monitor. Inoltre, è possibile creare script personalizzati da destinare alle principali aree di interesse. Nella pagina del TechCenter di Dell dedicata a Dell Command | Monitor sono disponibili alcuni script di esempio. Questi script possono essere utilizzati per monitorare l'inventario, le impostazioni del BIOS e lo stato del sistema.

- ① **N.B.:** L'installazione predefinita non abilita il supporto per SNMP. Per ulteriori informazioni sull'abilitazione del supporto per SNMP in Dell Command | Monitor per Windows, vedere la *Guida all'installazione di Dell Command | Monitor*, disponibile all'indirizzo [dell.com/dellclientcommandssuite/manuals](http://dell.com/dellclientcommandssuite/manuals).
- ① **N.B.:** L'installazione predefinita non abilita il supporto per SNMP. Per ulteriori informazioni sull'abilitazione del supporto per SNMP in Dell Command | Monitor per Windows, vedere la *Guida all'installazione di Dell Command | Monitor*.

# Conformità WSMT (Windows SMM Security Mitigations)

La tabella WSMT (Windows SMM Security Migrations) contiene informazioni sulla tabella ACPI che è stata creata per il sistema operativo Windows, che supporta le funzionalità di sicurezza basata sulla virtualizzazione (VBS). Dell Command | Monitor è compatibile con WSMT. Questa funzione viene utilizzata per configurare le caratteristiche della piattaforma sui sistemi client Dell con BIOS abilitata per WSMT.

Di seguito sono elencate le modifiche del comportamento dovute alla conformità WSMT:

- Le funzionalità di Dell Command | Monitor sono disponibili sulle piattaforme client Dell che hanno la versione BIOS compatibile con il supporto WMI/ACPI. Per maggiori informazioni sull'elenco di piattaforme, vedere [Piattaforme supportate](#).

## Caratteristiche

Le caratteristiche principali di Dell Command | Monitor sono:

- Supporto dello schema CIM
- Configurazione del BIOS
- Sicurezza WMI/OMI
- Segnalazione degli eventi
- Arresto remoto
- Accesso alle informazioni di sistema tramite lo schema CIM, utilizzando il protocollo WSMAN
- Compilazione di informazioni dettagliate sulle risorse.
- Configurabilità di attivazione remota
- Modifica remota delle impostazioni di sistema
- Il monitoraggio dello stato di integrità del sistema e stato dei rapporti
- Generazione di avvisi e monitoraggio RAID per i controller Intel ed LSI integrati.
- Monitoraggio e trap SNMP solo tramite Dell Command | Monitor per Windows

**❗ N.B.: Se si utilizza Dell Command | Monitor per Windows, le informazioni sono accessibili anche tramite SNMP.**

**❗ N.B.: Il monitoraggio dei controller Intel non è supportato per i sistemi Linux.**

### Supporto dello schema CIM

Dell Command | Monitor per Windows è conforme allo schema CIM 2.17 e include due provider WMI:

- Provider indicazione o agente di polling di WMI
- Istanza o provider metodo di WMI

Dell Command | Monitor per Linux è conforme allo schema CIM 2.32.0 e include due provider WMI:

- Provider indicazione o agente di polling di WMI
- Istanza o provider metodo di WMI

### Configurazione ed enumerazione delle impostazioni del BIOS

Dell Command | Monitor consente di configurare un BIOS di sistema.

### Sicurezza WMI/OMI

WMI provvede ad autenticare l'utente prima di concedere l'accesso a dati e metodi CIM. I privilegi di accesso vengono applicati dalla protezione DCOM (Distributed Component Object Model) e CIMOM. Agli utenti è consentito l'accesso completo o limitato per ciascuno spazio dei nomi. Non è prevista alcuna sicurezza a livello di proprietà o implementazione di classi. Per impostazione predefinita, gli utenti che fanno parte del gruppo di amministratori hanno accesso completo a WMI in locale e da remoto.

In Dell Command | Monitor per Windows la sicurezza WMI può essere configurata utilizzando il relativo controllo disponibile nella console di gestione del computer accessibile dalla sezione riservata a servizi e applicazioni. Fare clic con il pulsante destro del mouse su **Controllo**

**WMI**, quindi fare clic su **Proprietà**. È possibile configurare un livello di sicurezza specifico di uno spazio dei nomi dalla scheda **Sicurezza**. È inoltre possibile eseguire **Controllo WMI** dal menu **Start** o dalla **CLI** (Command Line Interface), eseguendo `wmimgmt.msc`.

## Segnalazione di avvisi

Dell Command | Monitor rileva gli eventi che si verificano nei sistemi Dell e avvisa l'utente locale e l'amministratore della rete riguardo a potenziali errori, modifiche alla configurazione, inventario dei componenti, controller RAID Intel ed LSI integrati, sensori e intrusioni. Questi eventi vengono visualizzati da un'applicazione per la gestione dei sistemi, ad esempio OpenManage Essentials (OME).

## Arresto remoto

Dell Command | Monitor per Windows supporta l'arresto e il riavvio del sistema da remoto.

## Accesso alle informazioni di sistema

Dell Command | Monitor consente di accedere alle informazioni sul sistema, ad esempio la versione e il produttore o il fornitore del BIOS, il codice di matricola, il modello del sistema e la data del primo utilizzo, tramite WMI/OMI in CIM. Per accedere alle informazioni tramite WMI/OMI è inoltre possibile utilizzare il protocollo WSMAN.

## Informazioni dettagliate sulle risorse

Dell Command | Monitor consente di accedere a informazioni dettagliate sull'inventario, come processori, dispositivi PCI e batterie.

## Configurazione di attivazione remota

Dell Command | Monitor supporta la configurazione di funzioni di riattivazione remota, una funzione del sistema client e della scheda di interfaccia di rete (NIC).

## Modifica da remoto delle impostazioni del BIOS del sistema

Dell Command | Monitor consente agli amministratori di recuperare e configurare le impostazioni del BIOS dei client aziendali, come la configurazione delle porte USB, le impostazioni delle NIC e così via.

## Integrità e stato del sistema

Dell Command | Monitor esegue il monitoraggio dell'integrità del sistema, ad esempio controllando lo stato della ventola, la memoria, la temperatura, la batteria, i problemi, i controller RAID e la docking station, per poi creare rapporti in merito.

## Monitoraggio e generazione di avvisi di RAID per controller Intel e LSI

Monitoraggio e creazione di avvisi relativi alle unità fisiche e logiche per i controller RAID Intel ed LSI in funzione di Dell Command | Monitor per Windows; monitoraggio e creazione di avvisi limitatamente ai controller LSI in funzione di Dell Command | Monitor per Linux.

Nel monitoraggio dello storage Dell Command | Monitor supporta il monitoraggio e la creazione di avvisi per:

- Il controller Intel integrato (compatibile con CSMI 0.81 o versione successiva)
- Controller RAID LSI integrati, 9217, 9271, 9341, 9361, 9440, 9460 e driver associati (fisici e logici)

 **N.B.: Il monitoraggio dei controller Intel non è supportato per i sistemi Linux.**

Per il monitoraggio dei sensori, Dell Command | Monitor supporta il monitoraggio e l'invio di avvisi dei sensori di tensione, temperatura, amperaggio, dispositivi di raffreddamento (ventola) e telaio.

## Monitoraggio e trap per SNMP

Dell Command | Monitor per Windows invia la conferma a SNMP v1 e supporta il monitoraggio di attributi e trap del sistema.

## Standard e protocolli.

Dell Command | Monitor è basato sugli standard CIM. La specifica CIM descrive in dettaglio le tecniche di mapping per una migliore compatibilità con i protocolli di gestione.

I protocolli di gestione, ad esempio WMI, SNMP e WSMAN, vengono utilizzati per il monitoraggio remoto.

**ⓘ N.B.: Dell Command | Monitor per Windows utilizza il protocollo Simple Network Management Protocol (SNMP) per descrivere diverse variabili del sistema.**

Il Desktop Management Task Force (DMTF) è il corpo di standard riconosciuti del settore che porta allo sviluppo, all'adozione e all'unificazione degli standard di gestione (inclusi CIM e ASF), e le iniziative per desktop, aziendali e degli ambienti Internet.

# Scenari utente

Questo capitolo descrive i vari scenari utente di Dell Command | Monitor.

Dell Command | Monitor può essere utilizzato per quanto segue:

- [Gestione delle risorse](#)
- [Gestione della configurazione](#)
- [Monitoraggio dello stato](#)
- [Profili](#)

Argomenti:

- [Scenario 1: gestione delle risorse](#)
- [Scenario 2: gestione della configurazione](#)
- [Scenario 3: monitoraggio dell'integrità](#)
- [Scenario 4: profili](#)

## Scenario 1: gestione delle risorse

Un'azienda con numerosi sistemi Dell non riesce a mantenere informazioni di inventario accurate a causa di cambiamenti a livello aziendale e del personale di IT. Il Chief Information Officer (CIO) richiede un piano per identificare i sistemi aggiornabili alle ultime versioni di Microsoft Windows. Si rende quindi necessaria una valutazione dei sistemi distribuiti per determinare le dimensioni, l'ambito e l'impatto finanziario di un progetto simile. Raccogliere le informazioni comporta un notevole sforzo. Assegnare il personale di IT a ogni sistema client ha dei costi notevoli in termini di ore/uomo e interruzioni degli utenti finali.

Utilizzando Dell Command | Monitor su ogni sistema di Dell, il responsabile dell'IT raccogliere velocemente le informazioni da remoto. Utilizzando strumenti come Microsoft System Center Configuration Manager (SCCM), il responsabile dell'IT interroga ogni sistema client tramite la rete e raccoglie informazioni come il tipo di CPU e la velocità, le dimensioni della memoria, la capacità del disco rigido, la versione del BIOS e la versione del sistema operativo in uso. Una volta raccolte le informazioni, possono essere analizzate per identificare i sistemi aggiornabili alla versione più recente di Windows.

È inoltre possibile ottenere un inventario delle risorse tramite la riga di comando WSMAN/WinRM o una riga di comando qualsiasi del client CIM.

## Integrazione di SCCM

Per integrare SCCM con Dell Command | Monitor per Windows:

- Utilizzare il file MOF nel pacchetto di installazione di Dell Command | Monitor, che contiene tutte le classi di Dell Command | Monitor, ed eseguire l'importazione in ConfigMgr.

Il MOF si trova in:

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

- Estensione delle funzionalità di creazione di rapporti sulle risorse utilizzando raccolte

## Scenario 2: gestione della configurazione

Un'azienda pianifica di standardizzare la piattaforma di client e di gestire ogni sistema per tutto il suo ciclo di vita. Per realizzare questi obiettivi, l'azienda acquisisce una suite di strumenti e prevede di automatizzare la distribuzione di un nuovo sistema operativo client utilizzando l'ambiente PXE (Preboot Execution Environment).

La sfida consiste nel modificare la password del BIOS di ciascun computer client, senza intervenire manualmente sul desktop. Installando Dell Command | Monitor su ogni sistema client, il reparto di IT aziendale può scegliere tra diverse opzioni per modificare l'ordine di avvio da remoto. OpenManage Essentials (OME) è una console di gestione integrabile in Dell Command | Monitor allo scopo di monitorare da remoto le impostazioni del BIOS di tutti i sistemi client dell'azienda. Un'altra opzione consiste nel creare uno script (CIM, WinRM/WSMAN/PowerShell/WMIC) per modificare le impostazioni del BIOS. Tale script può essere distribuito in rete da remoto ed eseguito su ogni sistema client.

Per ulteriori informazioni su Dell Command | Monitor, consultare la *Guida di riferimento di Dell Command | Monitor* all'indirizzo [dell.com/dellclientcommandsuite/manuals](https://dell.com/dellclientcommandsuite/manuals).

Per ulteriori informazioni su Dell Command | Monitor, consultare la *Guida di riferimento di Dell Command | Monitor*.

Le configurazioni standardizzate possono far risparmiare molto alle aziende di tutte le dimensioni. Molte organizzazioni distribuiscono sistemi client standardizzati, ma poche gestiscono la configurazione dei sistemi lungo il ciclo di vita di ogni computer. Installando Dell Command | Monitor in ciascun sistema client, il reparto di IT può bloccare le porte legacy per impedire l'utilizzo di periferiche non autorizzate oppure può abilitare la riattivazione LAN (WOL, Wake On LAN) per riattivare il sistema dallo stato di sospensione durante le ore non di punta e provvedere alle attività di gestione.

## Scenario 3: monitoraggio dell'integrità

Un utente riceve messaggi di errore di lettura durante il tentativo di accesso a determinati file sul disco rigido del sistema client. L'utente riavvia il sistema e sembra che i file siano ora accessibili. L'utente non tiene conto del problema iniziale perché sembra che si sia risolto da solo. Nel frattempo, Dell Command | Monitor interroga il disco rigido sul problema per un errore previsto e invia un avviso di Self-Monitoring, Analysis and Reporting Technology (SMART, Tecnologia di monitoraggio, analisi e segnalazione automatici) alla console di gestione. Inoltre mostra l'errore SMART all'utente locale. L'avviso indica che diversi errori di lettura/scrittura sono in corso nel disco rigido. Il reparto IT dell'azienda consiglia all'utente di eseguire immediatamente un backup dei file critici di dati. Un tecnico del servizio viene inviato con un'unità sostitutiva.

Il disco rigido viene sostituito prima che subisca un guasto, impedendo tempi di inattività per gli utenti, una chiamata all'helpdesk e la visita di un tecnico al desktop per diagnosticare il problema.

## Avvisi del sistema di monitoraggio mediante Visualizzatore eventi, Syslog, o indicazioni CIM del sistema operativo

Dell Command | Monitor supporta il monitoraggio degli eventi tramite le seguenti procedure:

- Estrazione del log tramite la classe CIM **DCIM\_LogEntry**.
- Monitoraggio dell'indicazione CIM tramite la classe **DCIM\_AlertIndication**.
- (Solo per Dell Command | Monitor per Windows) Monitoraggio degli eventi tramite protocollo SNMP (Simple Network Management Protocol) e Visualizzatore eventi di Windows.
- (Solo per Dell Command | Monitor per Linux) Monitoraggio tramite Syslog.

Per ulteriori informazioni su Dell Command | Monitor, consultare la *Guida di riferimento di Dell Command | Monitor* all'indirizzo [dell.com/dellclientcommandsuite/manuals](https://dell.com/dellclientcommandsuite/manuals).

Per ulteriori informazioni su Dell Command | Monitor, consultare la *Guida di riferimento di Dell Command | Monitor*.

# Scenario 4: profili

**ⓘ | N.B.: I profili DMTF vengono implementati solo per Dell Command | Monitor per Windows.**

Gli amministratori di IT sono chiamati a gestire i sistemi client in ambienti aziendali distribuiti e multifornitore. La difficoltà risiede nel dover gestire un insieme eterogeneo di strumenti e applicazioni, accanto a svariati sistemi desktop e client portatili in varie reti. Per ridurre il costo di questi requisiti e rappresentare i dati di gestione forniti, in Dell Command | Monitor sono implementati gli standard di settore DMTF (Distributed Management Task Force) e DCIM-OEM (Data Center Infrastructure Management). Alcuni dei profili di DMTF sono illustrati in questa guida.

Per ulteriori informazioni su Dell Command | Monitor, consultare la *Guida di riferimento di Dell Command | Monitor* all'indirizzo [dell.com/dellclientcommandsuitemanuals](https://dell.com/dellclientcommandsuitemanuals).

Per ulteriori informazioni su Dell Command | Monitor, consultare la *Guida di riferimento di Client Command | Monitor*.

## Profilo batteria

- Determinare lo stato della batteria enumerando o acquisendo l'istanza della classe **DCIM\_Battery**.
- Determinare il tempo di esecuzione stimato e vedere il livello di carica rimanente stimato.
- Controllare se le informazioni relative allo stato della batteria possono essere determinate utilizzando le proprietà *Stato operativo* e *HealthState* della classe **DCIM\_Battery**.
- Ottenere ulteriori informazioni relative allo stato di una batteria utilizzando la proprietà **DCIM\_Sensor.CurrentState** o la proprietà **CIM\_NumericSensor.CurrentState**.

## Profilo di gestione del BIOS

- Determinare la versione del BIOS enumerando l'istanza della classe **DCIM\_BIOSElement..**
- Controllare se i valori degli attributi del BIOS possono essere modificati o meno. Ottenere l'istanza della classe, **DCIM\_BIOSEnumeration**. L'attributo può essere modificato se la proprietà **IsReadOnly** è impostata su FALSO.
- Impostare la password di sistema (SystemPwd). Eseguire il metodo **DCIM\_BIOSService.SetBIOSAttributes()** e impostare la SystemPwd su AttributeName e il valore della password sui parametri di AttributeValue.
- Impostare la password del BIOS o Amministratore (AdminPwd). Eseguire il metodo **DCIM\_BIOSService.SetBIOSAttributes()** e impostare l'AdminPwd su AttributeName e il valore della password sui parametri di AttributeValue.
- Eseguire il metodo **DCIM\_BIOSService.SetBIOSAttributes()** e specificare i parametri di AttributeName e AttributeValue.
- Per modificare un attributo del BIOS quando la password del BIOS o Amministratore sono impostate, eseguire il metodo **DCIM\_BIOSService.SetBIOSAttributes()** e specificare AttributeName, AttributeValue e la password attuale del BIOS come parametro di input di AuthorizationToken.

## Controllo dell'avvio

- Modificare la sequenza degli elementi di avvio nell'elenco di avvio Legacy e UEFI.
- Abilitare o disabilitare gli elementi di avvio nell'elenco di avvio Legacy e UEFI.
- Trovare l'attuale configurazione di avvio enumerando le istanze della classe **DCIM\_ElementSettingData** la cui proprietà **IsCurrent** è impostata su **1**. Il **DCIM\_BootConfigSetting** rappresenta l'attuale configurazione di avvio.

## Base Desktop Mobile

- Determinare il modello del sistema, il numero di servizio e il numero di serie enumerando l'istanza della classe, **DCIM\_ComputerSystem**.
- Eseguire il metodo **DCIM\_ComputerSystem.RequestStateChange()** e impostare il valore del parametro RequestedState a **3**. Spegnere il sistema.

- Riavviare il sistema. Eseguire il metodo **DCIM\_ComputerSystem.RequestStateChange()** e impostare il valore del parametro **RequestedState** a **11**.
- Determinare lo stato di alimentazione del sistema.
- Determinare il numero di processori nel sistema interrogando **DCIM\_Processor**, le istanze che sono associate con l'istanza centrale tramite l'associazione **DCIM\_SystemDevice**.
- Ottenere l'ora del sistema. Eseguire il metodo **DCIM\_TimeService.ManageTime()** e impostare il parametro **GetRequest** su **Vero**.
- Controllare lo stato di integrità dell'elemento gestito.

## Record del registro

- Identificare il nome del registro selezionando l'istanza **DCIM\_RecordLog** in cui la proprietà **ElementName** corrisponde al nome del registro.
- Trovare le singole voci di registro. Ottenere tutte le istanze di **DCIM\_LogEntry** che sono associate con l'istanza data di **DCIM\_RecordLog** tramite l'associazione **DCIM\_LogManagesRecord**. Ordinare le istanze in base al **RecordID**.
- Controllare se i registri dei record sono abilitati o meno enumerando l'istanza della classe **DCIM\_RecordLog** la cui proprietà **Enabledstate** è impostata su **2** (cioè attivata) e **EnabledState** è impostata su **3** (cioè disabilitata).
- Ordinare i record dei registri in base all'indicazione di data e ora della voce di registro. Ottenere tutte le istanze di **DCIM\_LogEntry** che sono associate con l'istanza data di **DCIM\_RecordLog** tramite l'associazione **DCIM\_LogManagesRecord**. Ordinare le istanze di **DCIM\_LogEntry** in base al valore della proprietà **CreationTimeStamp** nell'ordine Last In First Out (LIFO).
- Cancellare i registri eseguendo il metodo **ClearLog()** per l'istanza data del **DCIM\_RecordLog**.

## Risorsa fisica

- Ottenere l'inventario fisico per tutti i dispositivi di un sistema.
- Ottenere l'inventario fisico per un telaio del sistema.
- Determinare il numero di parte di un componente danneggiato.
- Determinare se lo slot è vuoto o no.

## Profilo di memoria di sistema

- Ottenere le informazioni di memoria del sistema.
- Ottenere le informazioni della memoria fisica del sistema.
- Controllare la dimensione della memoria di sistema.
- Controllare la dimensione della memoria disponibile del sistema.
- Controllare la dimensione della memoria fisica del sistema.
- Controllare lo stato di integrità della memoria di sistema.

# Utilizzo di Dell Command | Monitor

Per visualizzare le informazioni fornite da Dell Command | Monitor, accedere al seguente percorso:

- `root\dcim\sysman (standard)`

Dell Command | Monitor fornisce le informazioni attraverso le classi in questi spazi dei nomi.

Per ulteriori informazioni sulle classi, consultare la *Dell Command | Monitor* all'indirizzo [dell.com/dellclientcommandsuitemanuals](http://dell.com/dellclientcommandsuitemanuals).

Per ulteriori informazioni sulle classi, consultare la *Dell Command | Monitor*.

Argomenti:

- [Impostazione dell'intervallo di polling](#)
- [Creazione di rapporti sullo stato del RAID](#)
- [Monitoraggio dei sistemi client Dell](#)
- [Registro applicazioni di Dell Command | Monitor per Linux](#)
- [Rilevamento delle unità del formato avanzato](#)
- [Configurazioni di avvio](#)
- [Modifica delle impostazioni audio](#)

## Impostazione dell'intervallo di polling

Utilizzando Dell Command Monitor, è possibile modificare l'intervallo di polling delle sonde della ventola, della temperatura, della tensione e della corrente, oltre che dell'aumento o della diminuzione della capacità del disco, della memoria e del numero di processori.

- In Windows il file `dcscopy32.ini` o `dcscopy64.ini` è disponibile al percorso `<percorso di installazione di Dell Command | Monitor>\omsa\ini`.
- In Linux il file `AlertPollingSettings.ini` è disponibile al percorso `/opt/dell/dcm/conf`.

**i** **N.B.:** I numeri nel file INI sono multipli di 23. L'intervallo di polling predefinito per la capacità del disco e gli avvisi della tecnologia SMART (Self-Monitoring, Analysis and Reporting Technology) è 626 secondi (tempo reale = 626 X 23 secondi, ovvero circa 3 ore).

## Creazione di rapporti sullo stato del RAID

Dell Command | Monitor abilita le informazioni di configurazione RAID ed esegue il monitoraggio del funzionamento del RAID nei sistemi client fornendo supporto per hardware e driver. È possibile utilizzare le classi RAID per ricevere i dettagli relativi a livelli RAID, informazioni sui driver, configurazione del controller e stato del controller. Al termine dell'abilitazione della configurazione RAID, sarà possibile ricevere gli avvisi per la riduzione delle prestazioni o guasti di unità e controller.

**i** **N.B.:** La creazione di rapporti sullo stato del RAID è supportata solo per i controller RAID che funzionano sui driver compatibili con Common Storage Management Interface (CSMI) versione 0.81. OMCI 8.1 e versioni successive supportano il monitoraggio solo nel controller RAID-on-Chip Intel; e OMCI 8.2 e versioni successive supportano gli avvisi per controller RAID-on-Chip Intel.

## Monitoraggio dei sistemi client Dell

- Dell Command | Monitor per Windows supporta il protocollo SNMP (Simple Network Management Protocol) per il monitoraggio e la gestione dei sistemi client, tra cui notebook, desktop e workstation. Il file MIB (Management Information Base) è condiviso tra Dell

Command | Monitor e l'amministratore del server. A partire dalla versione 9.0, Dell Command | Monitor per Windows è stato modificato in modo che utilizzi uno specifico OID client (10909) per consentire alle console di identificare i sistemi client.

Per ulteriori informazioni sul protocollo SNMP, consultare la *Guida di riferimento sul protocollo SNMP di Dell Command | Monitor*, disponibile all'indirizzo [dell.com/dellclientcommandsuitemanuals](http://dell.com/dellclientcommandsuitemanuals).

Per maggiori informazioni sul protocollo SNMP, consultare la *Guida di riferimento sul protocollo SNMP di Dell Command | Monitor*.

- Dell Command | Monitor per Linux supporta il monitoraggio tramite i comandi WinRM e WSMAN.

## Registro applicazioni di Dell Command | Monitor per Linux

Dell Command | Monitor per Linux separa i registri e gli avvisi delle applicazioni per la creazione di report e il debug. La cronologia di avvisi e registri generati per l'applicazione Dell Command | Monitor può essere visualizzata nel file **dcm\_application.log** disponibile al percorso `/opt/dell/dcm/var/log`.

## File di configurazione

È possibile aggiornare il file di configurazione **log.property** disponibile in `/opt/dell/dcm/conf` per applicare le impostazioni desiderate e il livello DEBUG:

**ⓘ | N.B.: Ogni volta che si modifica il file di configurazione, riavviare il server OMI per applicare le modifiche.**

- **Log\_Level.** I messaggi di sistema possono essere isolati nei tre livelli di registrazione ERROR, INFO e DEBUG

Il livello di registrazione può essere modificato dal file di configurazione. Se il livello di registrazione è impostato su DEBUG, l'applicazione Dell Command | Monitor invierà tutte le informazioni al file di registro specificato.

**ⓘ | N.B.: Per impostazione predefinita, il livello di registrazione è INFO.**

- **File\_Size.** L'utente può specificare le dimensioni massime del file **dcm\_application.log**. Per impostazione predefinita, il file ha 500 MB di dimensioni.

**ⓘ | N.B.: Il valore File\_Size deve essere espresso in byte.**

- **BackupIndex.** L'utente può specificare il conteggio di rollover del file **dcm\_application.log**. Se il conteggio di rollover predefinito è 2, il terzo file di backup andrà a sovrascrivere il file più vecchio.

## Rilevamento delle unità del formato avanzato

I sistemi client stanno migrando ad unità di Advanced Format (AF, formato avanzato) per una maggiore capacità di archiviazione e per superare le limitazioni dei dischi rigidi (HDD) con settore da 512 byte. I dischi rigidi che migrano a settori di 4 KB mantengono la compatibilità con le versioni precedenti, mentre l'attuale disco rigido AF, noto anche come disco rigido 512e, ha corrispondenza con SATA da 512 byte e opera a 4 KB. Durante la migrazione, è possibile incorrere in problemi di prestazioni, come unità di partizione non allineate nei sistemi client generando un errore di pacchetti software di crittografia basati su settori che gestiscono unità 512e. Dell Command | Monitor consente di determinare se il disco rigido in un sistema è un'unità AF a 4 KB, che aiuta a prevenire tali problemi.

## Configurazioni di avvio

**ⓘ | N.B.: Dell Command | Monitor per Linux non offre funzionalità per la configurazione di avvio. Pertanto, questa sezione non si applica a Dell Command | Monitor per Linux.**

Un sistema client può avere uno dei due tipi di configurazione di avvio:

- Legacy (BIOS)
- UEFI

In Dell Command | Monitor la configurazione di avvio (Legacy o UEFI) è modellata in base alle seguenti classi:

- **DCIM\_ElementSettingData**
- **DCIM\_BootConfigSetting**
- **DCIM\_OrderedComponent**
- **DCIM\_BootSourceSetting**

① **N.B.:** I termini "Configurazione di avvio" e "Tipo di elenco di avvio" sono intercambiabili e trasmettono il medesimo significato che rappresenta Legacy o UEFI.

## DCIM\_BootConfigSetting

Un'istanza di **DCIM\_BootConfigSetting** rappresenta una configurazione di avvio che viene utilizzata durante il processo di avvio. Ad esempio, su sistemi client, vi sono due tipi di configurazioni di avvio - Legacy e UEFI. In questo modo, **DCIM\_BootConfigSetting** ha un massimo di due istanze da dichiarare, una ciascuna per Legacy e UEFI.

È possibile determinare se **DCIM\_BootConfigSetting** dichiara Legacy, utilizzando le seguenti proprietà:

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

È possibile determinare se **DCIM\_BootConfigSetting** dichiara UEFI, utilizzando le seguenti proprietà:

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

## DCIM\_BootSourceSetting

Questa classe dichiara i dispositivi o le fonti di avvio. Le proprietà **ElementName**, **BIOSBootString** e **StructuredBootString** contengono una stringa che identifica i dispositivi di avvio. Ad esempio, floppy, disco rigido, CD/DVD, rete, Personal Computer Memory Card International Association (PCMCIA), veicolo elettrico a batteria (BEV) o USB. In base al tipo di elenco di avvio del dispositivo, un'istanza di **DCIM\_BootSourceSetting** è associata a una delle istanze di **DCIM\_BootConfigSetting**.

## DCIM\_OrderedComponent

La classe di associazione **DCIM\_OrderedComponent** viene usata per associare istanze di **DCIM\_BootConfigSetting** con istanze di **DCIM\_BootSourceSetting** che rappresentano uno dei tipi di elenco di avvio (Legacy o UEFI) a cui appartengono i dispositivi di avvio. La proprietà di **GroupComponent** di **DCIM\_OrderedComponent** si riferisce all'istanza **DCIM\_BootConfigSetting** e la proprietà di **PartComponent** si riferisce all'istanza **DCIM\_BootSourceSetting**.

## Modifica delle impostazioni audio

In Dell Command | Monitor utilizzare i seguenti metodi per modificare le impostazioni di sistema e lo stato del sistema locale o remoto:

- **SetBIOSAttributes**, per modificare le impostazioni del BIOS.
- ① **N.B.:** Al momento Dell Command | Monitor per Linux supporta solo il metodo **SetBIOSAttributes**.
- **ChangeBootOrder**, per modificare la configurazione di avvio.
- **RequestStateChange**, per arrestare e riavviare il sistema.
- **ManageTime**, per visualizzare l'ora di sistema.

In Dell Command | Monitor per Windows questi metodi sono eseguibili utilizzando winrm, script VB, i comandi PowerShell, wmic e WMI wbemtest.

# Impostazione degli attributi del BIOS in un sistema Windows che utilizza i comandi PowerShell

Per impostare gli attributi del BIOS, è possibile utilizzare il metodo SetBIOSAttributes. La procedura è descritta di seguito, utilizzando come esempio l'attività di abilitazione di Trusted Platform Module (TPM).

**❗ N.B.: Accertarsi che l'opzione TPM venga eliminata nel BIOS prima di seguire la procedura per abilitare il TPM.**

**❗ N.B.: Utilizzare PowerShell con privilegi di amministratore.**

Per attivare TPM:

- 1 Impostare la password del BIOS sul sistema se non è già stata impostata utilizzando il seguente comando PowerShell:  

```
Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSService | Invoke-CimMethod -MethodName SetBIOSAttributes -Arguments @{AttributeName=@"AdminPwd"};AttributeValue=@"<Admin password>"}
```
- 2 Abilitare la protezione TPM utilizzando il seguente comando:  

```
Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSService | Invoke-CimMethod -MethodName SetBIOSAttributes -Arguments @{AttributeName=@"Trusted Platform Module"};AttributeValue=@"1";AuthorizationToken="<Admin password>"}
```
- 3 Riavviare il sistema.
- 4 Attivare TPM utilizzando il seguente comando:  

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

# Impostazione degli attributi del BIOS nel sistema Linux

Per impostare gli attributi del BIOS, è possibile applicare uno dei seguenti metodi:

- [Utilizzo di OMICLI](#)
- [Utilizzo di WinRM](#)
- [Utilizzo di WSMAN](#)

**❗ N.B.: Controllare che il server OMI sia avviato e funzionante.**

## Impostazione degli attributi del BIOS tramite OMICLI

Per impostare gli attributi del BIOS, è possibile utilizzare il metodo SetBIOSAttributes. La procedura è descritta di seguito, utilizzando come esempio l'attività di abilitazione di Trusted Platform Module (TPM).

**❗ N.B.: Accertarsi che l'opzione TPM venga eliminata nel BIOS prima di seguire la procedura per abilitare il TPM.**

Per impostare gli attributi del BIOS utilizzando i comandi OMICLI:

- 1 Se non è ancora impostata, impostare la password del BIOS di sistema eseguendo  

```
./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 Per abilitare la sicurezza TPM, eseguire il seguente comando  

```
./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 Riavviare il sistema.

4 Per attivare TPM, eseguire

```
./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 Riavviare il sistema.

6 Per reimpostare la password del BIOS, eseguire

```
./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>" }
```

## Impostazione degli attributi del BIOS tramite WinRM

Per impostare gli attributi del BIOS, è possibile utilizzare il metodo SetBIOSAttributes. La procedura è descritta di seguito, utilizzando come esempio l'attività di abilitazione di Trusted Platform Module (TPM). Per i dettagli vedere [Gestione remota dei sistemi client di Dell](#).

**❗ N.B.: Accertarsi che l'opzione TPM venga eliminata nel BIOS prima di seguire la procedura per abilitare il TPM.**

Per impostare gli attributi del BIOS utilizzando i comandi WinRM:

1 Impostare il selettore elencando la classe DCIM\_BIOSService. Eseguire:

```
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
```

**❗ N.B.: Per l'operazione di impostazione illustrata in questo esempio verranno utilizzati i valori impostati per il selettore (SystemName=<nome sistema ricavato dalla classe DCIM\_BIOSService>winrm i SetBIOSAttributes wsman/DCIM\_BIOSService?SystemName=dt: +SystemCreationClassName=DCIM\_ComputerSystem+Name=DCIM:BiosService +CreationClassName=DCIM\_BIOSService+).**

2 Impostare la password del BIOS sul sistema se non è già stata impostata utilizzando il seguente 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 Abilitare la protezione TPM eseguendo questo 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 Riavviare il sistema.

5 Attivare TPM utilizzando il seguente 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>"}
```

## Impostazione degli attributi del BIOS tramite WSMAN

Nei sistemi che eseguono Linux è possibile impostare gli attributi del BIOS utilizzando WSMAN. La procedura è descritta di seguito, utilizzando come esempio l'attività di abilitazione di Trusted Platform Module (TPM). Per i dettagli vedere [Gestione remota dei sistemi client di Dell](#).

**❗ N.B.: Accertarsi che l'opzione TPM venga eliminata nel BIOS prima di seguire la procedura per abilitare il TPM.**

1 Impostare il selettore elencando la classe DCIM\_BIOSService. Eseguire:

```
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 Impostare la password del BIOS sul sistema se non è già stata impostata utilizzando il seguente 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 Abilitare la protezione TPM utilizzando il seguente 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 Riavviare il sistema.

5 Attivare TPM utilizzando il seguente 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>"
```

## Modifica dell'ordine di avvio

Per modificare la sequenza di avvio seguire i seguenti passaggi:

:

1 **Verificare il tipo di ordine di avvio (Legacy o UEFI) utilizzando il seguente comando:**

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

2 **Verificare il tipo di ordine di avvio corrente (Legacy o UEFI) utilizzando il seguente comando:**

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

3 **Modifica dell'ordine di avvio tramite il seguente comando:**

- 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")` .

**❶ N.B.: L'istanza `dcim_BootConfigSetting` deve rappresentare la configurazione di avvio che si desidera modificare: tipo 1 (Legacy) o tipo 2 (UEFI).**

- Gli argomenti sono i seguenti:
  - `AuthorizationToken` - Si tratta della password dell'amministratore o di avvio.
  - `Source` - Si tratta dell'elenco degli ordini di avvio derivante dalla proprietà `dcim_OrderedComponent.PartComponent`. Il nuovo ordine di avvio viene determinato dall'ordine delle unità di avvio nell'array di origine.

#### 4 Modifica dell'ordine di avvio per l'elenco di avvii del tipo 1 tramite PowerShell:

- Ottenere l'ordine di avvio corrente per l'elenco di avvii del tipo 1 utilizzando il seguente comando: `$boLegacy = gwmi -namespace root\dcim\sysman -class dcim_orderedcomponent | where {$_.partcomponent -match 'BootListType-1'} | select -expand partcomponent`.
- Definire una variabile PowerShell per specificare l'ordine di avvio per impostare `$newboLegacy`. Assegnare il nuovo ordine di avvio a quest'ultimo. Ad esempio, il tipo di ordine di avvio corrente viene mantenuto.
- `$newboLegacy = $boLegacy`
- Ottenere l'istanza `dcim_bootconfigsetting` corrispondente all'elenco di avvii del tipo 1 utilizzando il seguente comando: `$bcsLegacy = Gwmi -Namespace root\dcim\sysman -ClassName dcim_bootconfigsetting | where {$_.ElementName -eq 'Next Boot Configuration Setting : Boot List Type 1'}`.
- Richiamare il metodo utilizzando il seguente comando: `$ bcsLegacy.changebootorder($newboLegacy, $AuthorizationToken)`. La variabile `$AuthorizationToken` viene utilizzata per inviare la password del BIOS.

#### 5 Modifica dell'ordine di avvio per l'elenco di avvii del tipo 2 tramite PowerShell:

- Ottenere l'ordine di avvio corrente per l'elenco di avvii del tipo 2 utilizzando il seguente comando: `$boUefi = gwmi -namespace root\dcim\sysman -class dcim_orderedcomponent | where {$_.partcomponent -match 'BootListType-2'} | select -expand partcomponent`.
- Definire una variabile PowerShell per specificare l'ordine di avvio per impostare `$newboUefi`. Assegnare il nuovo ordine di avvio a quest'ultimo. Ad esempio, il tipo di ordine di avvio corrente viene mantenuto.
- Ottenere l'istanza `dcim_bootconfigsetting` corrispondente all'elenco di avvii del tipo 2 utilizzando il seguente comando: `$bcsUefi = Gwmi -Namespace root\dcim\sysman -ClassName dcim_bootconfigsetting | where {$_.ElementName -eq 'Next Boot Configuration Setting : Boot List Type 2'}`.
- Richiamare il metodo utilizzando il seguente comando: `$ bcsUefi.changebootorder($newboUefi, $AuthorizationToken)`. La variabile `$AuthorizationToken` viene utilizzata per inviare la password del BIOS.

## Arresto e riavvio del sistema operativo Windows da remoto

Il sistema operativo Windows può essere arrestato o riavviato da remoto utilizzando il metodo `RequestStateChange`.

- 1 Per arrestare Windows da remoto, utilizzare il seguente comando:

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

- 2 Per riavviare Windows da remoto, utilizzare il seguente comando:

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

## Come ottenere il valore dell'intervallo di tempo da remoto su un sistema Windows

Per ottenere da remoto il valore dell'intervallo di tempo del sistema operativo Windows, è possibile utilizzare il metodo `ManageTime`. Per esempio:

Nell'interfaccia della riga di comando, eseguire le seguenti operazioni:

- `$cred = Get-Credential`
- `$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"}
```

# Gestione dei sistemi client Dell a livello locale

I sistemi client Dell possono essere gestiti a livello locale con i seguenti metodi:

- Per i sistemi che eseguono Windows, è possibile [utilizzare PowerShell](#).
- Per i sistemi che eseguono Linux, è possibile [utilizzare OMICLI](#).

Argomenti:

- [Gestione locale dei sistemi Windows tramite PowerShell](#)
- [Gestione locale dei sistemi Linux tramite OMICLI](#)

## Gestione locale dei sistemi Windows tramite PowerShell

I sistemi client di Dell che eseguono Windows possono essere gestiti a livello locale utilizzando i comandi PowerShell.

- **Elenco delle istanze della classe DCIM**

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

- **Come ottenere le proprietà di un'impostazione del BIOS**

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

- **Modifica delle impostazioni del BIOS**

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

- **Modifica di valori non critici**

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

- **Sottoscrizione di avvisi**

```
$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)
```

## Gestione locale dei sistemi Linux tramite OMICLI

I sistemi Linux possono essere gestiti a livello locale utilizzando i comandi OMICLI. Nei sistemi che eseguono Linux, OMICLI è disponibile al percorso `/opt/omi/bin`.

- **Elenco delle istanze della classe DCIM**

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

- **Come ottenere le proprietà di un'impostazione del BIOS**

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

- **Impostazione della password di amministratore**

```
./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 }
```

- **Modifica delle impostazioni 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> }
```

- **Sottoscrizione di avvisi**

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

# Gestione remota dei sistemi client di Dell

I sistemi client Dell possono essere gestiti da remoto applicando uno dei seguenti metodi:

- Nei sistemi che eseguono Windows, [Gestione da remoto del sistema Windows tramite Windows PowerShell](#)
- Nei sistemi che eseguono Linux, [Gestione remota del sistema Linux tramite un sistema Windows che utilizza WinRM](#)

Argomenti:

- [Gestione da remoto del sistema Windows tramite Windows PowerShell](#)
- [Gestione remota del sistema Linux tramite un sistema Windows che utilizza WinRM](#)
- [Gestione remota del sistema Linux tramite un sistema Linux che utilizza WSMAN](#)

## Gestione da remoto del sistema Windows tramite Windows PowerShell

È possibile accedere al sistema Windows da remoto e monitorarlo utilizzando Windows PowerShell.

### Prerequisiti per la gestione del sistema Windows:

- Windows PowerShell 3.0
- PowerShell configurata per l'esecuzione di script remoti

### Prerequisiti per il sistema Windows gestito:

- Dell Command | Monitor.
- Windows PowerShell 3,0
- PowerShell configurata per l'esecuzione di script remoti
- Funzione PowerShell-remoting abilitata.

#### ① N.B.:

Per utilizzare Windows PowerShell in remoto, il computer remoto deve essere configurato per la gestione remota. Per ulteriori informazioni, tra cui le istruzioni, eseguire il comando PowerShell - `Get-Help about_remote_requirements`.

## Gestione remota del sistema Linux tramite un sistema Windows che utilizza WinRM

Utilizzando i comandi WinRM, è possibile accedere al sistema operativo Linux e monitorarlo tramite il sistema che esegue Microsoft Windows.

### Prerequisiti per il sistema operativo Windows

- Sistema operativo Windows supportato.
- Servizi WinRM in esecuzione e configurati per la gestione remota

### Prerequisiti per il sistema Linux

- Privilegi root
- Dell Command | Monitor.

- Sistema operativo Linux supportato.
- Abilitare le porte 5985 e 5986 sul server WMI
- Sistema configurato per l'ambiente.

Nell'interfaccia della riga di comando eseguire

```
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
```

## Gestione remota del sistema Linux tramite un sistema Linux che utilizza WSMAN

Utilizzando i comandi WSMAN, è possibile accedere al sistema operativo Linux da remoto e monitorarlo tramite il sistema che esegue Linux.

### Prerequisiti per la gestione del sistema Linux:

- Installazione del pacchetto del sistema operativo Linux supportato.
- Installazione del pacchetto wsmancli.

### Prerequisiti per il sistema Linux gestito:

- Privilegi di accesso root.
- Sistema operativo Linux supportato.
- Dell Command | Monitor

Avviare un terminale ed eseguire

```
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
```

## Domande frequenti

### Come si trova l'ordine di avvio (sequenza) della configurazione di avvio utilizzando la proprietà `DCIM_OrderedComponent.AssignedSequence`?

Quando un'istanza `DCIM_BootConfigSetting` (Legacy o UEFI) è associata a più istanze `DCIM_BootSourceSetting` (dispositivi di avvio) tramite istanze dell'associazione `DCIM_OrderedComponent`, il valore della proprietà `DCIM_OrderedComponent.AssignedSequence` viene utilizzato per stabilire la sequenza di utilizzo delle istanze `DCIM_BootSourceSetting` (dispositivi di avvio) associate durante il processo di avvio. Un'istanza `DCIM_BootSourceSetting` la cui proprietà associata `CIM_OrderedComponent.AssignedSequence` è uguale a `0` viene ignorata e non viene considerata parte dell'ordine di avvio.

### Come si modifica l'ordine di avvio?

L'ordine di avvio può essere modificato tramite il metodo `DCIM_BootConfigSetting.ChangeBootOrder()`. Il metodo `ChangeBootOrder()` imposta l'ordine in cui le istanze di `DCIM_BootSourceSetting` sono associate a una istanza `DCIM_BootConfigSetting`. Il metodo ha un parametro di input: **Origine**. Il parametro **Origine** è un array ordinato di proprietà **PartComponent** dalla classe `DCIM_OrderedComponent` che rappresenta l'associazione tra le istanze (dispositivi di avvio) `DCIM_BootSourceSetting` e l'istanza (tipo di elenco di avvio-Legacy o UEFI) `DCIM_BootConfigSetting`.

### Come si disabilitano i dispositivi di avvio?

Modificando l'ordine di avvio, il valore della proprietà **AssignedSequence** su ciascuna istanza di `DCIM_OrderedComponent`, che associa l'istanza di destinazione `DCIM_BootConfigSetting` con un'istanza `DCIM_BootSourceSetting` che non è presente nell'array di input del parametro **Origine**, è impostato su `0`, che indica che il dispositivo è disattivato.

### Quando ci si collega allo spazio dei nomi con `wbemtest`, viene visualizzato un messaggio di accesso non riuscito. Com'è possibile risolvere il problema?

Lanciare **wbemtest** con privilegi di amministratore per aggirare qualsivoglia messaggio di accesso. Accedere a Internet Explorer dall'elenco **Tutti i programmi**, fare clic con il pulsante destro del mouse su **Esegui come amministratore** per avviare **wbemtest** ed evitare possibili errori associati allo spazio dei nomi.

### Come posso eseguire gli script di TechCenter senza alcun problema?

Di seguito sono descritti i prerequisiti per eseguire gli script VBS forniti nel TechCenter di Dell Command | Monitor:

- 1 Configurare **winrm** nel sistema utilizzando il comando `winrm quickconfig`.
- 2 Verificare se il supporto del token esiste nel sistema facendo riferimento a:
  - La **schermata F2** nell'impostazione del BIOS.
  - Utilizzando uno strumento come **wbemtest** per verificare che il valore chiave definito nello script esista nel sistema.

① **N.B.:** Dell consiglia di utilizzare la versione più recente del BIOS, disponibile all'indirizzo [dell.com/support](http://dell.com/support). Per ulteriori informazioni, consultare la Guida di riferimento di Dell Command | Monitor all'indirizzo [dell.com/dellclientcommandssuitemanuals](http://dell.com/dellclientcommandssuitemanuals).

① **N.B.:** Utilizzare la versione più recente del BIOS disponibile.

## Come si impostano gli attributi del BIOS?

Gli attributi del BIOS possono essere modificati utilizzando il metodo **DCIM\_BIOSService.SetBIOSAttributes()**. Il metodo **SetBIOSAttributes()** imposta il valore dell'istanza definita nella classe **DCIM\_BIOSEnumeration**. Il metodo presenta sette parametri di input. I primi due parametri possono avere valore vuoto o Null. Il terzo parametro **AttributeName** deve eseguire il mapping dell'input al valore dell'istanza del nome attributo della classe **DCIM\_BIOSEnumeration**. Il quarto parametro o **AttributeValue** può essere uno qualsiasi dei possibili valori di **AttributeName**, come definito nella classe **DCIM\_BIOSEnumeration**. Se nel sistema è impostata la password del BIOS, occorre indicarla nel quinto argomento. Il sesto e il settimo argomento possono essere anch'essi vuoti o Null.

## Dell Command | Monitor supporta il monitoraggio di storage e sensori per i sistemi operativi Windows e Linux?

Sì, Dell Command | Monitor supporta il monitoraggio di storage e sensori per i sistemi operativi Windows e Linux supportati.

Nel monitoraggio dello storage Dell Command | Monitor supporta il monitoraggio e la creazione di avvisi per:

- Il controller Intel integrato (compatibile con CSMI 0.81 o versione successiva)
- Controller RAID LSI integrati; e 9217, 9271, 9341, 9361 e i driver associati (fisici e logici)

① **N.B.:** Il monitoraggio del controller Intel integrato non è supportato nei sistemi operativi Linux.

Per il monitoraggio dei sensori, Dell Command | Monitor supporta il monitoraggio e l'invio di avvisi dei sensori di tensione, temperatura, amperaggio, dispositivi di raffreddamento (ventola) e telaio.

Per ulteriori informazioni sulle classi e l'invio di avvisi, consultare la Guida di riferimento di Dell Command | Monitor all'indirizzo [dell.com/dellclientcommandssuitemanuals](http://dell.com/dellclientcommandssuitemanuals).

## È possibile integrare Dell Command | Monitor con altre applicazioni/console?

Sì, Dell Command | Monitor interagisce con le principali console di gestione aziendali che supportano gli standard del settore. Gli strumenti di gestione aziendale con cui può essere integrato sono:

- Dell Client Integration Suite per System Center 2012
- Dell OpenManage Essentials
- Dell Client Management Pack per System Center Operation Manager

## È possibile importare le classi in SCCM per l'inventario?

Sì, file MOF o OMCI\_SMS\_DEF.mof singoli possono essere importati nella console SCCM per l'inventario.

## Dove si trova il file SCCM OMCI\_SMS\_DEF.mof?

Il file OMCI\_SMS\_DEF.mof si trova sotto C:\Program Files\Dell\Command\_Monitor\ssa\omacim\OMCI\_SMS\_DEF.mof.



## Risoluzione dei problemi

Argomenti:

- Impossibile eseguire la connessione remota a Strumentazione gestione Windows
- Errore di installazione sui sistemi che eseguono Windows
- Il valore di enumerazione delle impostazioni del BIOS è 1
- Errore di installazione HAPI dovuto a dipendenze da libsmbios
- Le risorse CIM non sono disponibili
- Impossibile eseguire i comandi utilizzando DCM sui sistemi che eseguono Ubuntu Core 16

### Impossibile eseguire la connessione remota a Strumentazione gestione Windows

Se le informazioni Common Information Model (CIM) per un sistema di computer client remoto non è disponibile per l'applicazione di gestione o se un aggiornamento remoto del BIOS che utilizza Distributed Component Object Model (DCOM) non funziona, vengono visualizzati i seguenti messaggi di errore:

- **Accesso negato**
- **Il server Win32:RPC non è disponibile**

1 Controllare che il sistema client sia connesso alla rete. Digitare quanto segue nel prompt dei comandi del server:

```
ping <Host Name or IP Address> e premere <Enter>.
```

2 Eseguire la seguente procedura se sia il server che il sistema client si trovano nello stesso dominio:

- Verificare che l'account di amministratore di dominio disponga di privilegi di amministratore per entrambi i sistemi.

Eseguire la seguente procedura se sia il server che il sistema client sono in un gruppo di lavoro (non nello stesso dominio):

- Assicurarsi che il server sia in esecuzione sul server Windows più recente.

**i** **N.B.: Prima di modificare il registro, eseguire il backup dei file dei dati di sistema. Una modifica errata del registro potrebbe rendere inutilizzabile il sistema operativo.**

3 Correggere la modifica del registro sul sistema client. Fare clic su **Start > Esegui**, quindi digitare **regedit** e fare clic su **OK**. Nella finestra **Editor del Registro di sistema** accedere a **Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa**.

4 Impostare il valore **forceguest** su **0** (il valore predefinito è **1**). A meno che questo valore non venga modificato, l'utente che si connette al sistema da remoto avrà privilegi guest, anche se le credenziali fornite danno privilegi di amministratore.

- Creare un account sul sistema client con lo stesso nome utente e la password, come un account di amministratore del sistema in cui è in esecuzione l'applicazione di gestione di WMI.
- Se si utilizza IT Assistant, eseguire l'utilità ConfigServices al suo interno (**configservices.exe** nella directory **/bin** all'interno della directory di installazione di IT Assistant). Configurare l'esecuzione di IT Assistant in un account di amministratore locale, che a questo punto corrisponde anche all'amministratore del client remoto. Inoltre, verificare che siano abilitati DCOM e CIM.
- Se si utilizza IT Assistant, configurare tramite l'account amministratore il rilevamento della subnet per il sistema client. Inserire il nome utente nel formato **<nome computer client>\<nome account>**. Se il sistema è già stato rilevato, rimuoverlo dall'elenco dei sistemi rilevati, configurare il rilevamento della relativa subnet e quindi ripetere il rilevamento.

**i** **N.B.: Dell consiglia di utilizzare Dell OpenManage Essentials in sostituzione di IT Assistant. Per ulteriori informazioni su Dell OpenManage Essentials, visitare la pagina [dell.com/dellclientcommandsuite/manuals](http://dell.com/dellclientcommandsuite/manuals).**

**i** **N.B.: Utilizzare Dell OpenManage Essentials in sostituzione di IT Assistant.**

- 5 Eseguire la seguente procedura per modificare i livelli di privilegio dell'utente per la connessione remota a un WMI del sistema:
  - a Fare clic su **Start > Esegui**, digitare `compmgmt .msc`, quindi fare clic su **OK**.
  - b Sfoglia per **Controllo WMI** in **Servizi e applicazioni**.
  - c Fare clic con il pulsante destro del mouse su **Controllo WMI**, quindi fare clic su **Proprietà**.
  - d Fare clic sulla scheda **Sicurezza** e selezionare **DCIM/SYSMAN** sotto l'albero della **Directory principale**.
  - e Fare clic su **Sicurezza**.
  - f Selezionare il gruppo specifico o utente dei quali si desidera controllare l'accesso e usare le caselle di controllo **Consenti** o **Nega** per configurare le autorizzazioni.
- 6 Eseguire la seguente procedura per connettersi a WMI (`root\DCIM\SYSMAN`) da un sistema remoto utilizzando WMI CIM Studio:
  - a Installare **WMI Tools** insieme a `wbemtest` nel sistema locale, quindi installare Dell Command | Monitor nel sistema remoto.
  - b Configurare il firewall sul sistema per la connettività WMI remota. Ad esempio, aprire le porte TCP 135 e 445 nel firewall di Windows.
  - c Configurare l'impostazione **Protezione locale** su **Classica - Gli utenti locali si autenticano come se stessi per l'accesso alla rete: modello di condivisione e sicurezza per account locali** sotto **Criteri di protezione locali**.
  - d Connettersi alla WMI (`root\DCIM\sysman`) sul sistema locale da un sistema remoto utilizzando il `wbemtest` WMI. Ad esempio, `\\[Sistema remoto di destinazione]\root\DCIM\SYSMAN`.
  - e Immettere le credenziali di amministratore del sistema di destinazione remoto se richiesto.

Per ulteriori informazioni su WMI, consultare la documentazione Microsoft pertinente all'indirizzo [msdn.microsoft.com](http://msdn.microsoft.com).

## Errore di installazione sui sistemi che eseguono Windows

Se non è possibile completare l'installazione di Dell Command | Monitor per Windows, controllare che:

- L'utente disponga dei privilegi amministrativi nel sistema di destinazione.
- Il sistema di destinazione sia prodotto da Dell e disponga di SMBIOS 2.3 o versione successiva.
- La console PowerShell sia chiusa.

**❶ N.B.:** Per conoscere la versione di SMBIOS installata, fare clic su **Start > Esegui**, aprire il file `msinfo32.exe` e controllare la versione di SMBIOS nella pagina **Risorse di sistema**.

**❷ N.B.:** Nel sistema deve essere in esecuzione un sistema operativo Microsoft Windows supportato.

**❸ N.B.:** Il sistema deve essere aggiornato a NET 4.0 o versioni successive.

## Il valore di enumerazione delle impostazioni del BIOS è 1

- 1 Controllare di aver installato i seguenti pacchetti con privilegi di utente ROOT;
  - `omi-1.0.8.ssl_100.x64.rpm`
  - `srvadmin-hapi-8.3.0-1908.9058.el7.x86_64`
  - `command_monitor-linux-<numero versione>-<numero build>.x86_64.rpm`
- 2 Se i pacchetti sopra indicati sono installati, controllare che il modulo del driver sia stato caricato.
  - a Per farlo, eseguire il seguente comando `lsmod | grep dcdbas`.
  - b Se il modulo del driver non è disponibile, recuperare i dettagli del driver eseguendo il seguente comando `modinfo dcdbus`.
  - c Caricare il modulo del driver eseguendo il comando `insmod <filename>`.

## Errore di installazione HAPI dovuto a dipendenze da libsbios

Se l'installazione non riesce a causa di problemi relativi alle dipendenze,

forzare l'installazione di tutti i pacchetti dipendenti eseguendo `apt-get -f install`.

## Le risorse CIM non sono disponibili

In fase di enumerazione, se si riceve un errore simile a "Risorsa CIM non disponibile",

verificare che i comandi siano eseguiti con privilegi root.

## Impossibile eseguire i comandi utilizzando DCM sui sistemi che eseguono Ubuntu Core 16

Accertarsi che la versione Snap sul sistema sia la 2,23 o successiva.

## Altri documenti che potrebbero essere necessari

Oltre a questa Guida dell'utente, è possibile accedere ai seguenti documenti disponibili all'indirizzo **dell.com/dellclientcommandsuitemanuals**. Fare clic su Dell Command | Monitor (precedentemente OpenManage Client Instrumentation) e quindi fare clic sul collegamento appropriato della versione del prodotto nella sezione **Supporto generale**.

Oltre a questa Guida dell'utente, è anche possibile accedere alle seguenti guide.

- La *Guida di riferimento di Dell Command | Monitor* fornisce informazioni dettagliate su tutte le classi, proprietà e le descrizioni.
- La *Guida all'installazione di Dell Command | Monitor* fornisce informazioni sull'installazione.
- La *Guida di riferimento del protocollo SNMP di Dell Command | Monitor* fornisce MIB (Management Information Base) per il Simple Network Management Protocol (SNMP) applicabile a Dell Command | Monitor.

## Come contattare Dell

**❗ N.B.:** Se non si dispone di una connessione Internet attiva, è possibile trovare i recapiti sulla fattura di acquisto, sulla distinta di imballaggio, sulla fattura o sul catalogo dei prodotti Dell.

Dell offre diverse opzioni di servizio e assistenza telefonica e online. La disponibilità varia per paese e prodotto, e alcuni servizi potrebbero non essere disponibili nella vostra zona. Per contattare Dell per problemi relativi alla vendita, all'assistenza tecnica o all'assistenza clienti:

- 1 Accedere all'indirizzo Web **Dell.com/support**.
- 2 Selezionare la categoria di assistenza.
- 3 Verificare il proprio Paese nel menu a discesa **Scegli un Paese** nella parte inferiore della pagina.
- 4 Selezionare l'appropriato collegamento al servizio o all'assistenza in funzione delle specifiche esigenze.

Argomenti:

- [Altri documenti che potrebbero essere necessari](#)
- [Accesso ai documenti dal sito di supporto Dell EMC](#)

## Altri documenti che potrebbero essere necessari

Oltre a questa Guida dell'utente, è possibile accedere ai seguenti documenti disponibili all'indirizzo **dell.com/dellclientcommandsuitemanuals**. Fare clic su Dell Command | Monitor (precedentemente OpenManage Client Instrumentation) e quindi fare clic sul collegamento appropriato della versione del prodotto nella sezione **Supporto generale**.

Oltre a questa Guida dell'utente, è anche possibile accedere alle seguenti guide.

- La *Guida di riferimento di Dell Command | Monitor* fornisce informazioni dettagliate su tutte le classi, proprietà e le descrizioni.
- La *Guida all'installazione di Dell Command | Monitor* fornisce informazioni sull'installazione.
- La *Guida di riferimento del protocollo SNMP di Dell Command | Monitor* fornisce MIB (Management Information Base) per il Simple Network Management Protocol (SNMP) applicabile a Dell Command | Monitor.

## Accesso ai documenti dal sito di supporto Dell EMC

È possibile accedere ai documenti richiesti tramite uno dei seguenti link:

- Per i documenti di gestione dei sistemi aziendali Dell EMC - [Dell.com/SoftwareSecurityManuals](#)
- Per i documenti Dell EMC OpenManage - [Dell.com/OpenManageManuals](#)
- Per i documenti di gestione remota dei sistemi aziendali Dell EMC - [Dell.com/esmmanuals](#)
- Per i documenti di iDRAC e Dell EMC Lifecycle Controller - [Dell.com/idracmanuals](#)
- Per i documenti di gestione dei sistemi aziendali di connessione Dell EMC OpenManage - [Dell.com/OMConnectionsEnterpriseSystemsManagement](#)
- Per i documenti sugli strumenti di manutenzione Dell EMC - [Dell.com/ServiceabilityTools](#)
- a Accedere a [Dell.com/Support/Home](#).
- b Fare clic su **Scegli da tutti i prodotti**.
- c Dalla sezione **Tutti i prodotti** fare clic su **Software e sicurezza**, quindi fare clic sul collegamento richiesto da quanto segue:
  - **Gestione dei sistemi aziendali**

- **Gestione remota dei sistemi aziendali**
- **Strumenti di manutenzione**
- **Dell Client Command Suite**
- **Gestione dei sistemi client delle connessioni**

d Per visualizzare un documento, fare clic sulla versione di prodotto richiesta.

• Usando i motori di ricerca:

- Digitare il nome e la versione del documento nella casella di ricerca.