Dell Command | Monitor Versione 10.6

Guida per l'utente

Ottobre 2021
Rev. A01

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 evidenzia la possibilità che si verifichi un danno all'hardware o una perdita di dati ed indica come evitare il problema.

AVVERTENZA: un messaggio di AVVERTENZA evidenzia un potenziale rischio di danni alla proprietà, lesioni personali o morte.

Sommario

1

Introduzione a Dell Command | Monitor 10.6

L'applicazione software Dell Command | Monitor consente agli amministratori IT di gestire facilmente l'inventario del parco di PC, monitorare lo stato del sistema, modificare le impostazioni del BIOS e raccogliere informazioni in remoto per i sistemi client Dell implementati.

Il monitoraggio dello stato di integrità del sistema attivo può contribuire a ridurre i costi complessivi di gestione del sistema e rientra in un approccio olistico alla gestione di tutti i dispositivi in rete.

Dell Command | Monitor è progettato per i sistemi client Dell Enterprise, i sistemi gateway Dell IoT e i Dell Embedded PC.

Questo documento fornisce una panoramica su Dell Command | Monitor e sulle sue funzioni. Per ulteriori informazioni sui sistemi Dell supportati, fare riferimento alle note di rilascio disponibili all'indirizzo **dell.com/support**.

Argomenti:

Novità in questa versione di Dell Command | Monitor 10.6

- Supporto per i nuovi attributi BIOS riportati di seguito:
  - `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`
- Supporto del metodo **ResetBIOSDefaults**.

Dell Command | Monitor panoramica

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 dei protocolli di gestione Common Information Model (CIM) e il protocollo SNMP (Simple Network Management Protocol). Ciò consente di ridurre i costi complessivi di gestione del sistema, migliorare la sicurezza e fornire un approccio olistico per la gestione di tutti i dispositivi all'interno di un dispositivo di rete.

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

Dell Command | Monitor contiene il set di driver sottostanti che raccoglie le informazioni del sistema client da source differenti, tra cui il BIOS, il CMOS, il BIOS della gestione del sistema (SMBIOS), System Management Interface (SMI), il sistema operativo e l'interfaccia di programmazione delle applicazioni (API). Dell Command | Monitor per Windows raccoglie anche le informazioni di sistema client dalle Dynamic-Link Library (DLL) e dalle impostazioni di 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 Dell Knowledge Library 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.

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/support**.

2

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.

N.B.: Per maggiori informazioni sulle piattaforme supportate, vedere Piattaforme supportate.

3

Standard e protocolli per Dell Command | Monitor 10.6

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

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

N.B.: Dell Command | Monitor for Windows utilizza Simple Network Management Protocol (SNMP, Protocollo di gestione di rete semplice) per descrivere numerose 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 ambienti desktop, aziendali e Internet.

4

Scenari di casi d'uso di Dell Command | Monitor 10.6

Questo capitolo descrive i vari scenari di casi d'uso di Dell Command | Monitor.

È possibile utilizzare Dell Command | Monitor per:

- Gestione degli asset
- Gestione della configurazione
- Monitoraggio dello stato
- Profili

Argomenti:

Scenario 1: gestione degli asset

Una società che ha molti sistemi Dell non è stata in grado di mantenere informazioni di inventario accurate a causa di modifiche apportate al personale IT e all'azienda. Il Chief Information Officer (CIO) richiede un piano per l'identificazione dei sistemi che possono essere aggiornati alla versione più recente di Windows. Ciò richiede una valutazione dei sistemi implementati per determinare la dimensione, l'ambito e l'impatto finanziario di un progetto di questo tipo. La raccolta di informazioni prevede uno sforzo significativo. L'implementazione del personale IT su ciascun sistema client è costosa in termini di interruzioni per gli utenti finali.

Utilizzando Dell Command | Monitor su ciascun sistema Dell, il responsabile IT può raccogliere rapidamente le informazioni in remoto. Utilizzando strumenti come Microsoft System Center Configuration Manager (SCCM), il responsabile IT esegue una query su ciascun sistema client in rete e raccoglie informazioni quali tipo di CPU e velocità, dimensioni della memoria, capacità del disco rigido, versione BIOS e versione del sistema operativo corrente. Una volta raccolte, le informazioni possono essere analizzate per identificare i sistemi che possono essere aggiornati alla versione più recente di Windows.

È inoltre possibile ottenere l'inventario degli asset tramite la riga di comando di WSMAN/WinRM o la riga di comando di qualsiasi client CIM.

Integrazione di SCCM

È possibile integrare SCCM con Dell Command | Monitor per Windows mediante:

- Utilizzo del file MOF nel pacchetto di installazione di Dell Command | Monitor, che contiene tutte le classi di Dell Command | Monitor e l'importazione in ConfigMgr

  Il MOF si trova in:

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

- Estensione delle funzionalità di creazione di rapporti sugli asset 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 l'implementazione 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 su ciascun desktop. Installando Dell Command | Monitor su ogni sistema client, il dipartimento 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. 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/support**.

Le configurazioni standardizzate possono far risparmiare molto sui costi alle aziende di tutte le dimensioni. Molte organizzazioni implementano 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 dipartimento IT può bloccare le porte legacy per evitare l'uso di periferiche non autorizzate o abilitare la Riattivazione LAN (WOL) per riattivare il sistema da uno stato di sospensione durante le ore non di punta, in modo da eseguire le attività di gestione dei sistemi.

Scenario 3: monitoraggio dell'integrità

Un utente riceve messaggi di errore di lettura quando tenta di accedere a determinati file sul disco rigido del sistema client. L'utente riavvia il sistema e adesso sembra che i file siano accessibili. L'utente ignora il problema iniziale perché sembra essersi risolto. Nel frattempo, Dell Command | Monitor esegue una query sul disco rigido per un problema di errore previsto e invia un avviso SMART (Self-Monitoring, Analysis and Reporting Technology, Tecnologia di monitoraggio, analisi e segnalazione automatici) alla console di gestione. Inoltre, visualizza l'errore SMART anche all'utente locale. L'avviso indica che sono presenti più errori di lettura/scrittura nel disco rigido. Il dipartimento IT dell'azienda ha consigliato di eseguire immediatamente un backup dei file di dati critici dell'utente. Viene inviato un tecnico di assistenza con un'unità sostitutiva.

Il disco rigido viene sostituito prima che subisca un guasto, impedendo il downtime per gli utenti, una chiamata all'help desk 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 procedure riportate di seguito:

- 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/support**.

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 multi-vendor. 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/support**.

Profilo degli asset

Stato della garanzia sul dispositivo endpoint:

- Determinare lo stato della garanzia enumerando o acquisendo l'istanza della classe **DCIM_AssetWarrantyInformation**.
- Verificare se lo stato della garanzia può essere determinato utilizzando le proprietà **WarrantyStartDate** e **WarrantyEndDate** della classe **DCIM_AssetWarrantyInformation**.

  N.B.: Il prerequisito per DCIM_AssetWarrantyInformation è quello di disporre di una connessione Internet funzionante. Se si sta eseguendo Dell Command | Monitor dietro a un server proxy, accertarsi che le impostazioni proxy siano configurate correttamente.

  Per ottenere ulteriori informazioni sullo stato della garanzia delle periferiche:

  1. Visitare il sito Dell.com/support.
  2. Verificare il proprio Paese o regione nel menu a discesa Scegli un Paese/regione nella parte inferiore della pagina.
  3. Selezionare la categoria di supporto: Garanzia e contratti
  4. Fornire il codice di matricola del sistema
- Disabilitare la funzione di garanzia e le successive chiamate di refresh.
- Eseguire il pull delle informazioni sulla garanzia on-demand.

N.B.: Le informazioni sulla garanzia vengono aggiornate automaticamente ogni 15 giorni. In caso di stato sulla garanzia recente, le informazioni sulla garanzia enumerate potrebbero non essere uguali a quelle del sito del supporto Dell.

Profilo della 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**.
- Determinare la posizione della batteria e dell'ePPID della batteria utilizzando le proprietà **IdentifyingDescriptions** e **OtherIdentifyingInfo** della classe **DCIM_Battery**.

DCIM_Battery

Per ottenere le informazioni sul valore ePPID della batteria per un elemento della batteria. Aprire un prompt PowerShell con i privilegi di amministratore ed eseguire il comando `Get-CimInstance -Namespace root/dcim/sysman -Classname DCIM_Battery |Select ElementName, OtherIdentifyingInfo, IdentifyingDescriptions`.

N.B.: Il valore di ePPID della batteria non è dinamico e se la batteria è stata sostituita, è necessario riavviare il sistema per riflettere le modifiche nell'istanza **DCIM_Battery**.

Profilo di gestione del BIOS

- Determinare la versione del BIOS enumerando l'istanza della classe **DCIM_BIOSElement**.
- Verificare se i valori degli attributi del BIOS possono essere modificati o non. 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 SystemPwd su AttributeName e il valore della password sui parametri di AttributeValue.
- Impostare la password del BIOS o dell'amministratore (AdminPwd). Eseguire il metodo **DCIM_BIOSService.SetBIOSAttributes()** e impostare 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**. **DCIM_BootConfigSetting** rappresenta la configurazione di avvio corrente.

Base Desktop Mobile

- Determinare il modello del sistema, il codice di matricola e il numero di serie enumerando l'istanza della classe, **DCIM_ComputerSystem**.
- È possibile utilizzare il metodo **DCIM_ComputerSystem.RequestStateChange()** per impostare il valore del parametro RequestedState su **3**. Il valore del parametro 3 spegne il sistema.
- È possibile utilizzare il metodo **DCIM_ComputerSystem.RequestStateChange()** per impostare il valore del parametro **RequestedState** su **11**. Il valore del parametro 11 riavvia il sistema.
- 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.
- Individuare le singole voci di registro. Ottenere tutte le istanze di **DCIM_LogEntry** associate all'istanza specificata 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 di registro in base all'indicatore dell'ora della voce di registro. Ottenere tutte le istanze di **DCIM_LogEntry** associate all'istanza specificata di **DCIM_RecordLog** tramite l'associazione **DCIM_LogManagesRecord**. Ordinare le istanze di **DCIM_LogEntry** in base al valore della proprietà **CreationTimeStamp** in ordine LIFO (Last-In, First-Out).
- Cancellare i registri eseguendo il metodo **ClearLog()** per l'istanza data del **DCIM_RecordLog**.

Asset fisico

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

Profilo della 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.

5

Utilizzo di Dell Command | Monitor 10.6

È possibile visualizzare le informazioni fornite da Dell Command | Monitor accedendo a: `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 Guida di riferimento di Dell Command | Monitor all'indirizzo **dell.com/support**.

Argomenti:

Impostazione dell'intervallo di polling

È possibile modificare l'intervallo di polling di sonda della ventola, sonda della temperatura, sonda della tensione, sonda della corrente, aumento/diminuzione della capacità del disco, aumento/diminuzione delle dimensioni della memoria e aumento/diminuzione del numero di processori, utilizzando Dell Command | Monitor.

- Per Windows, il file `dcsbdy32.ini` o `dcsbdy64.ini` è presente in `<Dell Command | Monitor installed location>\omsa\ini`.
- Per Linux, il file `AlertPollingSettings.ini` è presente in `/opt/dell/dcm/conf`.

N.B.: I numeri nel file INI sono multipli di **23**. L'intervallo di polling predefinito per capacità del disco e avviso di Self-Monitoring, Analysis and Reporting Technology (SMART, Tecnologia di monitoraggio, analisi e segnalazione automatici) è **626** secondi (il tempo reale = 626 X 23 secondi, che sono circa 3 ore).

Creazione di rapporti sullo stato del RAID

Dell Command | Monitor abilita le informazioni di configurazione del RAID e monitora la funzionalità RAID per i sistemi client con supporto driver e hardware. 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.

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 il Server Administrator. Dell Command | Monitorper Windows dalla versione 9.0 è stato modificato in modo da utilizzare un OID che sia specifico per l'OID (10909) del client affinché le console individuino i sistemi client.

Per ulteriori informazioni su SNMP, consultare la Guida di riferimento di SNMP di Dell Command | Monitor all'indirizzo **dell.com/support**.

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

Registro applicazioni per Dell Command | Monitor per Linux

Dell Command | Monitor per Linux separa i registri e gli avvisi delle applicazioni per finalità di reporting e debug. La cronologia degli avvisi e dei registri generati per l'applicazione Dell Command | Monitor può essere visualizzata nel file **dcm_application.log** disponibile in `/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 per il DEBUG:

N.B.: Riavviare il server OMI dopo aver apportato eventuali modifiche al file di configurazione per applicare tali modifiche.

- Livello_Registro - Sono disponibili tre livelli di registro per separare i messaggi del sistema: ERRORE, INFO, DEBUG

  L'utente può modificare il livello di registro dal file di configurazione. Se il livello del registro è impostato su DEBUG, l'applicazione Dell Command | Monitor invierà tutte le informazioni nel file di registro specificato.

  N.B.: Il livello di registro predefinito è impostato su INFO.
- Dimensioni_File - L'utente può specificare le dimensioni massime del file **dcm_application.log**. La dimensione file predefinita è 500 MB.

  N.B.: Il valore di Dimensioni_File deve essere espresso in byte.
- BackupIndex - L'utente può specificare il numero di rollover del file **dcm_application.log**. Se il numero di rollover predefinito è 2, il terzo file di backup sovrascriverà il file meno recente.

Rilevamento delle unità del formato avanzato

I sistemi client stanno passando alle unità Advanced Format (AF) perché offrono maggiori capacità di storage e per evitare le limitazioni dei dischi rigidi (HDD) con settore a 512 byte. I dischi rigidi che passano a settori da 4 KB mantengono la compatibilità con le versioni precedenti, mentre gli attuali dischi rigidi AF, noti come dischi rigidi 512e, offrono SATA a 512 byte e operano a 4 KB. Durante la transizione, è possibile riscontrare problemi relativi alle prestazioni, come unità di partizione non allineate correttamente nei sistemi client che causano un guasto ai pacchetti software di crittografia basati su settore che gestiscono le 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 for Linux non offre la funzione di configurazione di avvio. Pertanto, questa sezione non è applicabile a Dell Command | Monitor for 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 utilizzando le seguenti classi:

- DCIM_ElementSettingData
- DCIM_BootConfigSetting
- DCIM_OrderedComponent
- DCIM_BootSourceSetting
- DCIM_SmartAttributeInfo

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_AssetWarrantyInformation

- Per interrogare lo stato della garanzia sul dispositivo endpoint, eseguire il seguente comando nel prompt PowerShell:

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

- Per elencare i diritti di garanzia in ordine cronologico di `WarrantyEndDate`, eseguire il comando che segue nel prompt PowerShell:

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

- Per disabilitare la funzione di garanzia e le successive chiamate di refresh, eseguire il comando che segue nel prompt PowerShell:

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

- Per eseguire il pull delle informazioni sulla garanzia on-demand, eseguire il comando che segue nel prompt PowerShell:

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

N.B.: impostazione della configurazione proxy:

- Proxy predefinito: Dell Command | Monitor seleziona il proxy di sistema predefinito (impostato in IE)
- Proxy personalizzato

  La classe **DCIM_ApplicationProxySetting** viene utilizzata per modificare le impostazioni proxy per Dell Command | Monitor in base all'ambiente proxy.

DCIM_BootConfigSetting

Un'istanza di **DCIM_BootConfigSetting** rappresenta una configurazione di avvio utilizzata durante il processo di avvio. Ad esempio, sui sistemi client esistono due tipi di configurazioni di avvio: Legacy e UEFI. Quindi, **DCIM_BootConfigSetting** può rappresentare un massimo di due istanze: 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 rappresenta i dispositivi di avvio o source. Le proprietà **ElementName**, **BIOSBootString** e **StructuredBootString** contengono una stringa che identifica i dispositivi di avvio. Ad esempio, disco floppy, disco rigido, CD/DVD, rete, Personal Computer Memory Card International Association (PCMCIA), veicolo elettrico a batterie (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** è utilizzata per associare le istanze di **DCIM_BootConfigSetting** alle istanze di **DCIM_BootSourceSetting** che rappresentano uno dei tipi riportati nell'elenco di avvio (Legacy o UEFI) a cui appartiene il dispositivo di avvio. La proprietà **GroupComponent** di **DCIM_OrderedComponent** si riferisce all'istanza **DCIM_BootConfigSetting** e la proprietà **PartComponent** si riferisce all'istanza **DCIM_BootSourceSetting**.

Attributo DCIM_Smart

Per leggere il valore dell'attributo smart, eseguire i seguenti comandi:

Per esempio:

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

Per impostare i valori di soglia personalizzati, eseguire i seguenti comandi:

Per esempio:

- 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 gestisce le impostazioni di configurazione termica come Thermal Mode, AAC Mode e Fan Failure Mode.

- Per la querty delle informazioni termiche del dispositivo, eseguire il seguente comando:

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

- Per impostare il valore della modalità termica, eseguire il seguente 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")}
```

Modifica delle impostazioni di sistema

In Dell Command | Monitor, usare i seguenti metodi per modificare le impostazioni di sistema e lo stato dei sistemi locali o remoti:

- SetBIOSAttributes - Modifica le impostazioni del BIOS

  N.B.: Dell Command | Monitor per Linux attualmente supporta solo il metodo SetBIOSAttributes.
- ChangeBootOrder - Modifica la configurazione di avvio
- RequestStateChange - arresta e riavvia il sistema
- ManageTime - Visualizza l'ora del sistema

In Dell Command | Monitor per Windows, è possibile eseguire questi metodi utilizzando script VB, WinRM, VB script, comandi PowerShell, wmic e WMI wbemtest.

Ripristino delle impostazioni predefinite del BIOS per i sistemi in cui è in esecuzione Windows o Linux

ResetBIOSDefaults (metodo)

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

Comando 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> }`

Valori possibili:

- 0-Predefiniti sicuri integrati: conosciuti anche come impostazioni predefinite del BIOS. Questa configurazione supporta qualsiasi piattaforma. Pertanto, la configurazione non può essere modificata.
- 1- Ultima configurazione valida: generata automaticamente dal BIOS una volta completato correttamente il POST. Questa opzione ripristina il BIOS all'ultima configurazione valida. Se i **predefiniti sicuri integrati** sono corrotti, è possibile utilizzare l'opzione **Ultima configurazione valida** per ripristinare il BIOS.

- 2-Impostazioni di fabbrica: le impostazioni di fabbrica vengono generate prima di inviare il sistema. Questa configurazione è ottimizzata per la configurazione hardware o personalizzata in base alle richieste dell'utente durante l'acquisto o il servizio.
- 3-Configurazione utente 1: configurata se richiesto dall'utente. È necessario selezionare **Salva configurazione corrente** nella configurazione del BIOS o nella schermata F2 per ripristinare la configurazione tramite l'applicazione Dell Command | Monitor.
- 4-Configurazione utente 2: configurata se richiesto dall'utente. È necessario selezionare **Salva configurazione corrente** nella configurazione del BIOS o nella schermata F2 per ripristinare la configurazione tramite l'applicazione Dell Command | Monitor.

Tabella 1. Possibili valori ResetBIOSDefaults

Descrizione	Codice errore (valore SetResult)
Operazione completata	0
Valore di input non valido/Valore di input non compreso nell'intervallo	1
Errore di autenticazione	2
Configurazione non supportata	3
Configurazione vuota	4
Errore generico/Operazione non riuscita/quando il servizio non è in esecuzione	4294967295

N.B.: È necessario riavviare il sistema dopo l'operazione **ResetBIOSDefaults** affinché le modifiche vengano applicate correttamente.

DCM Windows è in grado di arrestare o riavviare il sistema tramite le seguenti API:

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

Le seguenti API possono essere utilizzate nel sistema operativo GNU o Linux:

- shutdown -r +5
- sudo reboot

N.B.: durante l'operazione di ripristino, un sottoinsieme di opzioni non viene ripristinato alle impostazioni predefinite per motivi di sicurezza (ad esempio la password) o per la possibilità di avvio (ad esempio l'elenco di avvio e le ROM di opzione legacy).

I registri eventi del BIOS non vengono ripristinati per archiviare la cronologia dell'hardware di sistema.

La tabella seguente contiene l'elenco completo delle funzioni che non vengono ripristinate alle impostazioni predefinite.

Tabella 2. Elenco completo delle funzioni che non vengono ripristinate alle impostazioni predefinite

Sezione	Sottosezione	Elemento
Informazioni generali	Informazioni di sistema	Codice di matricola
	Informazioni di sistema	Codice asset
	Informazioni di sistema	Ownership Tag
	Sequenza di avvio	Elenco di avvio
	Advanced Boot Options	Attivazione OROM legacy
	Date/Time	Date/Time
	Scheda di rete integrata	Scheda di rete integrata
	Scheda di rete integrata	Enable UEFI Network Stack
	SATA Operation (Funzionamento SATA)	SATA Operation (Funzionamento SATA)
Sicurezza	NA	Admin Password
	NA	Password di sistema

Tabella 2. Elenco completo delle funzioni che non vengono ripristinate alle impostazioni predefinite (continua)

Sezione	Sottosezione	Elemento
	NA	Password HDD-x interno
	NA	Master Password Lockout
	SMM Security Mitigation	SMM Security Mitigation
	Intel SGX Enable	Intel SGX Enable
Secure Boot	Secure Boot Enable	Secure Boot Enable
	Expert Key Management	Key Databases

Impostazione degli attributi del BIOS in un sistema in cui è in esecuzione Windows utilizzando i comandi PowerShell

È possibile impostare gli attributi del BIOS utilizzando il metodo SetBIOSAttributes. La procedura viene descritta di seguito utilizzando un'attività per abilitare il Trusted Platform Module (TPM) come esempio.

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 il 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 sicurezza 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 il 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.

   Esclusione di responsabilità generica

   Il modulo Powershell PSReadline salva ogni comando console immesso in un file di testo. Pertanto, si consiglia di utilizzare il comandlet "Get-Credential" per gestire la password in modo sicuro.

   a. $cred = Get-Credential

   b. Immettere il nome utente e la password, ad esempio, AdminPWD e Dell_123$, quando viene visualizzata la finestra di dialogo.

   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 ")}

Impostazione degli attributi del BIOS nel sistema Linux

È possibile impostare gli attributi del BIOS utilizzando uno dei seguenti metodi:

- Utilizzo di OMICLI
- Utilizzo di WinRM

- Utilizzo di WSMan

N.B.: Accertarsi che il server OMI sia avviato e in esecuzione.

Impostazione degli attributi del BIOS tramite OMICLI

È possibile impostare gli attributi del BIOS utilizzando il metodo SetBIOSAttributes. La procedura viene descritta di seguito utilizzando un'attività per abilitare il Trusted Platform Module (TPM) come esempio.

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 tramite i comandi OMICLI:

1. Per impostare la password del BIOS nel sistema se non è già impostata, 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 "<new Admin Password>" }
```

2. Per abilitare la sicurezza TPM utilizzare il seguente comando ed 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" AttributeValue "1" AuthorizationToken
"<password>"
```

3. Riavviare il sistema.
4. Per attivare il 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

È possibile impostare gli attributi del BIOS utilizzando il metodo SetBIOSAttributes. La procedura viene descritta di seguito utilizzando un'attività per abilitare il Trusted Platform Module (TPM) come esempio.

N.B.: accertarsi che l'opzione TPM sia deselezionata nel BIOS prima di seguire la procedura per abilitare il TPM.

Per impostare gli attributi del BIOS tramite i comandi WinRM:

1. Impostare il selettore enumerando 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.: i valori impostati dal selettore (SystemName=<system name from DCIM_BIOSService class>winrm i SetBIOSAttributes wsman/DCIM_BIOSService?SystemName=dt:

+SystemCreationClassName=DCIM_ComputerSystem+Name=DCIM:BiosService+CreationClassName=DCIM_BIOSService+) vengono usati per impostare le operazioni in questo esempio.

2. Impostare la password del BIOS nel 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 sicurezza TPM eseguendo 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";AttributeValue="1";AuthorizationToken="<Admin password>"}
```

4. Riavviare il sistema.
5. Attivare il 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

È possibile impostare gli attributi del BIOS sui sistemi in cui è in esecuzione Linux tramite WSMan. La procedura viene descritta di seguito utilizzando un'attività per abilitare il Trusted Platform Module (TPM) come esempio.

N.B.: accertarsi che l'opzione TPM sia deselezionata nel BIOS prima di seguire la procedura per abilitare il TPM.

1. Impostare il selettore enumerando 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 nel 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 sicurezza 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 il 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: `Get-WmiObject -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: `Get-WmiObject -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: `(Get-WmiObject -namespace root\dcim\sysman -class dcim_bootconfigsetting).getmethodparameters("ChangeBootOrder") .`

     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:
     - `Authorization Token` - 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:
   a. Ottenere l'ordine di avvio corrente per l'elenco di avvii del tipo 1 utilizzando il seguente comando: `$boLegacy = Get-WmiObject -namespace root\dcim\sysman -class dcim_orderedcomponent | where {$_.partcomponent -match 'BootListType-1'} | select -expand partcomponent.`
   b. 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.
   c. $newboLegacy = $boLegacy
   d. Ottenere l'istanza `dcim_bootconfigsetting` corrispondente all'elenco di avvii del tipo 1 eseguendo il seguente comando: `$bcsLegacy = Get-WmiObject -Namespace root\dcim\sysman -ClassName dcim_bootconfigsetting | where {$_.ElementName -eq 'Next Boot Configuration Setting : Boot List Type 1'}.`
   e. Richiamare il metodo eseguendo il seguente comando: `$ 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:
   a. Ottenere l'ordine di avvio corrente per l'elenco di avvii del tipo 2 utilizzando il seguente comando: `$boUefi = Get-WmiObject -namespace root\dcim\sysman -class dcim_orderedcomponent | where {$_.partcomponent -match 'BootListType-2'} | select -expand partcomponent.`
   b. Definire una variabile PowerShell per specificare l'ordine di avvio per impostare `$newboUefi`. Assegnare il nuovo ordine di avvio a quest'ultimo. Ad esempio, il tipo di ordine di avvio corrente viene mantenuto.
   c. Ottenere l'istanza `dcim_bootconfigsetting` corrispondente all'elenco di avvii del tipo 2 eseguendo il seguente comando: `$bcsUefi = Get-WmiObject -Namespace root\dcim\sysman -ClassName dcim_bootconfigsetting | where {$_.ElementName -eq 'Next Boot Configuration Setting : Boot List Type 2'}.`

d. Richiamare il metodo eseguendo il seguente comando: `$ bcsUefi.changebootorder($newboUefi, $AuthorizationToken)`. La variabile `$AuthorizationToken` viene utilizzata per inviare la password del BIOS.

Arresto e riavvio del sistema Windows da remoto

È possibile arrestare o riavviare il sistema Windows in remoto utilizzando il metodo RequestStateChange.

1. Arrestare il sistema Windows in remoto utilizzando il seguente comando:

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

2. Riavviare il sistema Windows in remoto utilizzando il seguente comando:

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

Come ottenere il valore del tempo del sistema nel sistema Windows in remoto

È possibile ottenere il valore del tempo del sistema per il sistema Windows in remoto utilizzando il metodo ManageTime. Per esempio:

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

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"}`

6

Gestione locale dei sistemi client Dell tramite Dell Command | Monitor 10.6

È possibile gestire i sistemi client Dell localmente utilizzando i seguenti metodi:

- Per i sistemi su cui è in esecuzione Windows, utilizzando PowerShell
- Per i sistemi su cui è in esecuzione Linux, utilizzando OMICLI

Argomenti:

Gestione locale dei sistemi Windows tramite PowerShell

È possibile gestire localmente i sistemi client Dell su cui è in esecuzione Windows utilizzando i comandi PowerShell.

- Enumerazione delle istanze della classe DCIM
  - `Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSEnumeration`
  - `Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSPassword`
- Recupero delle proprietà per 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 degli 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)
```

- Comandi per ottenere il consenso dell'utente dalla WMI:

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

- Comandi per impostare il consenso dell'utente dalla WMI:

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

N.B.: Il programma di miglioramento per Dell Command | Monitor è disponibile per le versioni 10.5 e 10.6 a x64 bit.

- Comandi per ottenere il proxy dalla WMI:

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

- Comandi per impostare il proxy dalla WMI:

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

Gestione locale dei sistemi Linux tramite OMICLI

È possibile gestire i sistemi Linux localmente utilizzando i comandi OMICLI. Nei sistemi in cui è in esecuzione Linux, OMICLI viene installato in `/opt/omi/bin`.

- Enumerazione delle istanze della classe DCIM
  - `./omicli ei root/dcim/sysman DCIM_BIOSEnumeration`
  - `./omicli ei root/dcim/sysman DCIM_BIOSPassword`
- Recupero delle proprietà per un'impostazione del BIOS

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

- Impostazione della password Admin

```
./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 degli avvisi

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

7

Gestione remota dei sistemi client Dell utilizzando Dell Command | Monitor 10.6

È possibile gestire i sistemi client Dell in remoto utilizzando uno dei seguenti metodi:

- Per i sistemi su cui è in esecuzione Windows, Gestione remota del sistema Windows tramite sistema Windows utilizzando PowerShell a pagina 25
- Pei sistemi in cui è in esecuzione Linux Gestione remota del sistema Linux tramite un sistema Windows che utilizza WinRM a pagina 25

Argomenti:

Gestione remota del sistema Windows tramite sistema Windows utilizzando PowerShell

È possibile accedere e monitorare il sistema Windows in remoto tramite un sistema Windows utilizzando PowerShell.

Prerequisiti per il sistema Windows di gestione:

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

Prerequisiti per il sistema Windows gestito:

- Dell Command | Monitor
- Windows PowerShell 3.0
- PowerShell configurato per l'esecuzione di script remoti
- La funzione PowerShell da remoto deve essere abilitata

N.B.:

Per utilizzare Windows PowerShell in remoto, è necessario configurare il computer remoto per la gestione remota. Per ulteriori informazioni, incluse le istruzioni, eseguire il comando PowerShell – `Get-Help` about_Remote_Requirements.

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

È possibile accedere e monitorare il sistema su cui è in esecuzione Linux tramite il sistema che esegue Windows utilizzando i comandi WinRM.

Prerequisiti per il sistema Windows

- Sistemi operativi Windows supportati
- Servizi WinRM in esecuzione e configurati per la gestione remota

Prerequisiti per il sistema Linux

- Privilegi root
- Dell Command | Monitor
- Sistemi operativi Linux supportati
- 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

È possibile accedere e monitorare il sistema su cui è in esecuzione Linux tramite un sistema che esegue Linux utilizzando i comandi WSMan.

Prerequisiti per il sistema di gestione Linux:

- Il pacchetto del sistema operativo Linux supportato è installato
- Il pacchetto wsmancli è installato

Prerequisiti per il sistema Linux gestito:

- Privilegi di accesso root
- Sistemi operativi Linux supportati
- 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
```

8

Domande frequenti su Dell Command | Monitor 10.6

- 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.

- Il messaggio di accesso non riuscito viene visualizzato quando <dispositivo che tenta di connettersi> tenta di connettersi al namespace con wbemtest.

  Lanciare **wbemtest** con privilegi di amministratore per aggirare qualsivoglia messaggio di accesso. Accedere a Internet Explorer dall'elenco **Tutti i programmi**, cliccare con il pulsante destro del mouse su **Esegui come amministratore** per avviare **wbemtest** ed evitare errori associati al namespace.

- Come posso eseguire gli script di Knowledge Library senza alcun problema?

  Di seguito sono descritti i passaggi per eseguire gli script VBS forniti nel link alla Knowledge Library di Dell Command | Monitor:

  1. Configurare **winrm** nel sistema utilizzando il comando `winrm quickconfig`.
  2. Verificare se il supporto del token esiste nel sistema consultando:
     - La **schermata F2** nell'impostazione del BIOS.
     - Utilizzando uno strumento come wbemtest per verificare che i valori chiave definiti nello script esistano nel sistema.

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

- 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**. Il quinto parametro AuthorizationToken è opzionale, l'immissione del quinto parametro è la password del BIOS. Il quinto parametro viene utilizzato solo se la password del BIOS è impostata, altrimenti è vuoto. 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)

- I controller RAID LSI integrati; e 9217, 9271, 9341, 9361 e i driver associati (fisici e logici)

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

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

Per ulteriori informazioni sulle classi e sull'invio di avvisi, consultare la Guida di riferimento di Dell Command | Monitor all'indirizzo **dell.com/support**.

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

  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 in C:\Program Files\Dell\Command_Monitor\ssa\omacim\OMCI_SMS_DEF.mof.
- Come configurare il proxy per DCM 10.2.1?
- DCM 10.2.1 non è in grado di recuperare le informazioni sulla garanzia.
- Verificare che le impostazioni del proxy dell'applicazione siano configurate correttamente utilizzando la classe DCIM_ApplicationProxySetting.

  Come configurare le credenziali proxy per Dell Command | Monitor.

  Se l'utente ha effettuato l'accesso tramite Dell Command | Monitor, può utilizzare le stesse credenziali per l'autenticazione proxy.
- Dell Command | Monitor non visualizza le informazioni sulla garanzia.
  - Il sistema client non è connesso a Internet durante il polling.

    Connettersi a Internet ed eseguire il pull delle informazioni sulla garanzia eseguendo il comando `Get-CimInstance -Namespace root/DCIM/SYSMAN -ClassName DCIM_AssetWarrantyInformation| Where-Object{$_.InstanceID -eq "Root/MainSystemChassis/COOObject/COOWarranty:0"} | Invoke-CimMethod -MethodName RefreshWarranty`
  - Il sistema client non è configurato con il server proxy.

    Configurare le impostazioni proxy in Dell Command | Monitor eseguendo i seguenti comandi:

    - Per ottenere il proxy da WMI, eseguire il comando `Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_ApplicationProxySetting`.
    - Per impostare il proxy da WMI, eseguire il comando `Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_ApplicationProxySetting | Invoke-CimMethod -MethodName Change ProxySetting -Arguments @{NewAddress="10.0.0.223"; NewPort="8080"}`

      Sostituire **NewAddress** e **NewPort** in base all'ambiente proxy (se applicabile).

9

Procedure di risoluzione dei problemi di Dell Command | Monitor 10.6

Argomenti:

Impossibile eseguire la connessione remota a Strumentazione gestione Windows

Se le informazioni Common Information Model (CIM) per un sistema di computer client remoto non sono disponibili 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. Verificare 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 esegua la versione più recente di Windows Server.

   N.B.: Eseguire il backup dei file di dati di sistema prima di modificare il registro di sistema. La modifica errata del registro di sistema potrebbe rendere inutilizzabile il sistema operativo.
3. Apportare la modifica del registro di sistema sul sistema client. Cliccare su **Start** > **Esegui**, digitare **regedit**, quindi cliccare su **OK**. Nella finestra **Editor del registro di sistema**, accedere a `My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`.
4. Impostare il valore di **forceguest** su 0 (il valore predefinito è 1). A meno che non si modifichi questo valore, l'utente che si connette in remoto al sistema avrà i privilegi guest, anche se le credenziali fornite danno privilegi di amministratore.
   a. Creare un account sul sistema client con lo stesso nome utente e password, come un account di amministratore del sistema in cui è in esecuzione l'applicazione di gestione di WMI.
   b. Se si utilizza IT Assistant, eseguire l'utilità IT Assistant ConfigServices (`configservices.exe` nella directory `/bin` all'interno della directory di installazione di IT Assistant). Configurare IT Assistant affinché venga eseguito con un account amministratore locale, che ora è anche amministratore sul client remoto. Inoltre, verificare che DCOM e CIM siano abilitati.
   c. Se si utilizza IT Assistant, utilizzare l'account di amministratore per configurare la rilevazione della subnet per il sistema client. Inserire il nome utente come <nome computer client>\<nome account>. Se il sistema è già stato rilevato, rimuovere il sistema dall'elenco dei sistemi rilevati, configurare la rilevazione della subnet e quindi ripetere la rilevazione.

   N.B.: Dell consiglia di utilizzare Dell OpenManage Essentials in sostituzione di IT Assistant. Per ulteriori informazioni su Dell OpenManage Essentials, consultare **dell.com/support**.
5. Eseguire la seguente procedura per modificare i livelli di privilegio dell'utente per la connessione remota a un WMI del sistema:
   a. Cliccare su **Start** > **Esegui**, digitare `compmgmt.msc`, quindi cliccare su **OK**.
   b. Accedere a **Controllo WMI** in **Servizi e applicazioni**.

c. Cliccare con il pulsante destro del mouse su **Controllo WMI**, quindi cliccare su **Proprietà**.
d. Cliccare sulla scheda **Sicurezza** e selezionare **DCIM/SYSMAN** nella struttura **Directory principale**.
e. Cliccare su **Sicurezza**.
f. Selezionare il gruppo o l'utente specifico del quale 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 un WMI (`root\DCIM\SYSMAN`) su un sistema da un sistema remoto utilizzando WMI CIM Studio:
   a. Installare strumenti di WMI insieme a wbemtest nel sistema locale, quindi installare Dell Command | Monitor nel sistema remoto.
   b. Configurare il firewall sul sistema per la connettività remota WMI. Ad esempio, aprire le porte TCP 135 e 445 in Windows Firewall.
   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** in **Criteri di protezione locali**.
   d. Connettersi al WMI (`root\DCIM\SYSMAN`) sul sistema locale da un sistema remoto utilizzando WMI wbemtest. Ad esempio, \\[Indirizzo IP del 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.

Errore di installazione nei sistemi in cui è in esecuzione Windows

Se non si è in grado di completare l'installazione di Dell Command | Monitor per Windows, verificare che:

- L'utente disponga dei privilegi amministrativi nel sistema di destinazione.
- Il sistema di destinazione sia un sistema Dell con SMBIOS aggiornato alla versione 2.3 o successiva.
- PowerShell Console non sia aperta.

N.B.: Per visualizzare la versione SMBIOS del sistema, andare a **Start** > **Esegui** ed eseguire il file `msinfo32.exe`. Controllare la versione di SMBIOS nella pagina Risorse di sistema.

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

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

Il valore di enumerazione delle impostazioni del BIOS visualizzato è 1

1. Verificare che i seguenti pacchetti siano installati 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-<version number>-<buid number>.x86_64.rpm
2. Se sono installati i pacchetti di cui sopra, verificare che il modulo del driver sia caricato.
   a. Per verificare che il modulo del driver sia caricato, 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 seguente comando `insmod <filename>`.

Installazione HAPI non riuscita a causa della dipendenza da libsmbios

Se l'installazione fallisce a causa di problemi di dipendenza,

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

Risorse CIM non disponibili

Durante l'enumerazione, se si riceve un errore come "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 sul sistema sia installata la versione snap 2.23 o successiva.

10

Altri documenti che potrebbero essere necessari

Oltre a questa Guida per l'utente, è possibile accedere ai seguenti documenti disponibili all'indirizzo **dell.com/support**. Cliccare su Dell Command | Monitor (precedentemente OpenManage Client Instrumentation), quindi cliccare sul link appropriato della versione del prodotto nella sezione **Supporto generale**.

Oltre a questa Guida per l'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.

Argomenti:

Accesso ai documenti dal sito di supporto Dell

È possibile accedere ai documenti richiesti selezionando il prodotto.

1. Visitare il sito www.dell.com/manuals.
2. Cliccare su **Visualizza tutti i prodotti**, cliccare su **Software**, quindi su **Client Systems Management**.
3. Per visualizzare i documenti richiesti, cliccare sul nome del prodotto e sul numero di versione richiesti.

11

Come contattare Dell

N.B.: Se non si dispone di una connessione a Internet attiva, le informazioni sui contatti sono reperibili anche 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. Visitare il sito **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 link al servizio o all'assistenza in funzione delle specifiche esigenze.