

Dell Command | Monitor Versie 10.6

Gebruikershandleiding



Opmerkingen, voorzorgsmaatregelen, en waarschuwingen

 **OPMERKING:** Een OPMERKING duidt belangrijke informatie aan voor een beter gebruik van het product.

 **WAARSCHUWING: WAARSCHUWINGEN duiden potentiële schade aan hardware of potentieel gegevensverlies aan en vertellen u hoe het probleem kan worden vermeden.**

 **GEVAAR: LET OP** duidt het risico van schade aan eigendommen, lichamelijk letsel of overlijden aan.

Inhoudsopgave

Hoofdstuk 1: Kennismaking met Dell Command Monitor 10.6	5
Nieuw in deze release van Dell Command Monitor 10.6	5
Dell Command Monitor Overzicht	5
Hoofdstuk 2: Windows SMM Security Mitigations Table (WSMT)-compatibiliteit	7
Hoofdstuk 3: Standaarden en protocollen voor Dell Command Monitor 10.6	8
Hoofdstuk 4: Gebruiksscenario's met Dell Command Monitor 10.6	9
Scenario 1: Asset management	9
SCCM-integratie	9
Scenario 2: Configuratiebeheer	9
Scenario 3: Statuscontrole	10
Systeemwaarschuwingen bewaken via Logboeken, Syslog of CIM-indicatie van het besturingssysteem	10
Scenario 4: Profielen	10
Assetprofiel	10
Batterijprofiel	11
Profiel BIOS-beheer	11
Opstartbeheer	11
Mobiel basisbureaublad	12
Logboekrecord	12
Fysieke asset	12
Profiel systeemgeheugen	12
Hoofdstuk 5: Dell Command Monitor 10.6 gebruiken	13
Polling-interval instellen	13
Statusrapportage RAID	13
De Dell clientsystemen controleren	13
Applicatielogboek voor Dell Command Monitor voor Linux	14
Stations met geavanceerde indeling detecteren	14
Opstartconfiguraties	14
DCIM_AssetWarrantyInformation	15
DCIM_BootConfigSetting	15
DCIM_BootSourceSetting	15
DCIM_OrderedComponent	15
DCIM_Smart kenmerk	16
DCIM_ThermalInformation	16
De systeeminstellingen wijzigen	16
Het BIOS opnieuw instellen op de standaardinstellingen voor Windows- of Linux-systemen	16
BIOS-kenmerken in een Windows-systeem instellen met behulp van PowerShell-opdrachten	18
BIOS-kenmerken instellen in het Linux-systeem	19
De opstartvolgorde wijzigen	21
Het Windows-systeem op afstand afsluiten en opnieuw opstarten	22
De systeemtijdwaarde voor een Windows-systeem op afstand ophalen	22

Hoofdstuk 6: Het lokale beheer van Dell clientsystemen via Dell Command Monitor 10.6.....	23
Windows-systemen lokaal beheren met PowerShell.....	23
Linux-systemen lokaal beheren met OMICLI.....	24
Hoofdstuk 7: Het beheer van Dell clientsystemen op afstand met behulp van Dell Command Monitor 10.6.....	25
Windows-systeem op afstand beheren met PowerShell.....	25
Linux-systeem beheren op afstand met Windows-systeem met WinRM.....	25
Linux-systeem op afstand beheren via een Linux-systeem met WSMAN.....	26
Hoofdstuk 8: Veelgestelde vragen over Dell Command Monitor 10.6.....	27
Hoofdstuk 9: Stappen voor probleemoplossing met behulp van Dell Command Monitor 10.6.....	29
Kan geen externe verbinding maken met Windows Management Instrumentation.....	29
Installatiefout op systemen waarop Windows wordt uitgevoerd.....	30
Inventarisatiewaarde van BIOS-instelling wordt weergegeven als 1.....	30
Hapi-installatie mislukt vanwege de afhankelijkheid van libsbios.....	31
CIM-resource niet beschikbaar.....	31
Kan opdrachten niet uitvoeren met behulp van DCM op de systemen met Ubuntu Core 16.....	31
Hoofdstuk 10: Andere documenten die u misschien nodig hebt.....	32
Documenten openen op de Dell supportwebsite.....	32
Hoofdstuk 11: Contact opnemen met Dell.....	33

Kennismaking met Dell Command | Monitor 10.6

Met de applicatie Dell Command | Monitor kunnen IT-administrators eenvoudig een inventaris van de apparatuur beheren, de systeemstatus bewaken, BIOS-instellingen wijzigen en op afstand informatie verzamelen voor geïmplementeerde Dell clientsystemen.

Actieve systeemstatusbewaking kan helpen de TCO (Total Cost of Ownership) van het systeem te verlagen en is onderdeel van een holistische aanpak voor het beheer van alle netwerkapparaten.

Dell Command | Monitor is ontworpen voor Dell Enterprise clientsystemen, Dell IoT Gateway-systemen en voor Dell Embedded pc's.

Dit document biedt een overzicht van Dell Command | Monitor en de functies daarvan. Zie voor meer informatie over ondersteunde Dell systemen de Releaseopmerkingen op dell.com/support.

Onderwerpen:

- [Nieuw in deze release van Dell Command | Monitor 10.6](#)
- [Dell Command | Monitor Overzicht](#)

Nieuw in deze release van Dell Command | Monitor 10.6

- Support voor de volgende nieuwe BIOS-kenmerken:
 - 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
- Ondersteuning voor de methode **ResetBIOSDefaults**.

Dell Command | Monitor Overzicht

OPMERKING: Simple Network Management Protocol (SNMP) wordt niet ondersteund voor Dell Command | Monitor voor Linux.

Dell Command | Monitor beheert clientsystemen met de beheerprotocollen Common Information Model (CIM)-standaard en het Simple Network Management Protocol (SNMP). Dit helpt om de TCO (Total Cost of Ownership) van het systeem te verlagen, de beveiliging te verbeteren en biedt een holistische aanpak voor het beheer van alle apparaten binnen een netwerk.


Door CIM te gebruiken kunt u Dell Command | Monitor openen via Web Services for Management Standards (WSMAN).

Dell Command | Monitor bevat de onderliggende set drivers die informatie over clientsystemen verzamelt uit verschillende bronnen, zoals het BIOS, CMOS, System Management BIOS (SMBIOS), System Management Interface (SMI), besturingssysteem en Application Programming Interfaces (API's). Dell Command | Monitor voor Windows verzamelt ook informatie over clientsystemen uit DLL's (Dynamic-Link Library) en registerinstellingen. Dell Command | Monitor voor Windows haalt deze informatie op via de CIM Object Manager-interface (CIMOM), via de Windows Management Instrumentation-stack (WMI) of via de SNMP-agent, terwijl Dell Command | Monitor voor Linux deze informatie ophaalt via de Open Management Infrastructure-interface (OMI).

Dell Command | Monitor biedt IT-administrators de mogelijkheid om asset-informatie te verzamelen, BIOS-instellingen te wijzigen, proactieve meldingen over mogelijke slechte omstandigheden te ontvangen en meldingen te krijgen over mogelijke inbreuken op de

beveiliging. In de Windows-systemen zijn deze meldingen beschikbaar als voorvallen in NT event log, in WMI event of in SNMP traps v1. Voor de Linuxsystemen worden deze meldingen ontvangen als Syslog, OMI event of applicatielog.

Dell Command | Monitor voor Windows kan worden geïntegreerd in een console zoals Microsoft System Center Configuration Manager door de CIM-informatie direct te openen, of door andere consoleleveranciers die de Dell Command | Monitor integratie hebben geïmplementeerd. Bovendien kunt u aangepaste scripts aanmaken voor de belangrijkste doelgebieden. Voorbeeldscripts zijn beschikbaar op de pagina Dell Command | Monitor van de Dell Knowledge Library. U kunt deze scripts gebruiken om de inventaris, de BIOS-instellingen en de systeemstatus te bewaken.

 **OPMERKING:** De standaardinstallatie schakelt geen SNMP-ondersteuning in. Zie voor meer informatie over het inschakelen van SNMP-ondersteuning voor Dell Command | Monitor voor Windows de Dell Command | Monitor installatiehandleiding op dell.com/support.

Windows SMM Security Mitigations Table (WSMT)-compatibiliteit

De Windows SMM Security Mitigations Table bevat informatie over de ACPI-tabel die is opgesteld voor het Windows-besturingssysteem, dat Windows Virtualization-Based Security (VBS)-functies ondersteunt. Dell Command | Monitor is WSMT-compatibel. Deze tabel wordt gebruikt voor het configureren van de platformfuncties op Dell clientsystemen met een BIOS waarin WSMT is ingeschakeld.

Hieronder vindt u de gedragswijziging die het gevolg is van WSMT-compatibiliteit:


Dell Command | Monitor-functies zijn beschikbaar op Dell clientplatformen die beschikken over de compatibele BIOS-versie die WMI/ACPI ondersteunt.

 **OPMERKING:** Zie [Ondersteunde platforms](#) voor meer informatie over de platformlijst.

Standaarden en protocollen voor Dell Command | Monitor 10.6

Dell Command | Monitor is gebaseerd op CIM-standaarden. De CIM-specificatie geeft een nauwkeurige beschrijving van toewijzingstechnieken voor een verbeterde compatibiliteit met beheerprotocollen.

Beheerprotocollen zoals WMI, SNMP en WSMAN worden gebruikt voor controle op afstand.

 **OPMERKING:** Dell Command | Monitor voor Windows gebruikt Simple Network Management Protocol (SNMP) om verschillende variabelen van het systeem te beschrijven.

De Desktop Management Task Force (DMTF) is het door de branche erkende normalisatie-instituut dat leiding geeft aan de ontwikkeling, aanvaarding en de unificatie van beheerstandaarden (inclusief CIM en ASK) en initiatieven voor desktop-, bedrijfs- en internetomgevingen.

Gebruiksscenario's met Dell Command | Monitor 10.6

Dit gedeelte beschrijft de verschillende gebruiksscenario's van Dell Command | Monitor.

U kunt Dell Command | Monitor gebruiken voor:

- [Asset management](#)
- [Configuratiebeheer](#)
- [Statuscontrole](#)
- [Profielen](#)

Onderwerpen:

- [Scenario 1: Asset management](#)
- [Scenario 2: Configuratiebeheer](#)
- [Scenario 3: Statuscontrole](#)
- [Scenario 4: Profielen](#)

Scenario 1: Asset management

Een bedrijf dat veel Dell systemen heeft, kon geen nauwkeurige asset-informatie bijhouden vanwege veranderingen in het bedrijf en IT-personeel. De Chief Information Officer (CIO) vraagt een plan voor het identificeren van de systemen die kunnen worden geüpgraded naar de nieuwste versie van Windows. Dit vereist een evaluatie van geïmplementeerde systemen om de omvang, reikwijdte en financiële impact van een dergelijk project te bepalen. De informatieverzameling vergt een aanzienlijke inspanning. Het inzetten van IT-personeel op elk clientsysteem is duur in termen van onderbrekingen voor de eindgebruiker.

Met Dell Command | Monitor op elk Dell systeem kan de IT-manager snel informatie op afstand verzamelen. Met tools zoals Microsoft System Center Configuration Manager (SCCM) wordt door de IT-manager via het netwerk een query uitgevoerd op elk clientsysteem en wordt informatie verzameld zoals CPU-type en -snelheid, geheugengrootte, hardeschijfcapaciteit, BIOS-versie en huidige besturingssysteemversie. Nadat de informatie is verzameld, kan deze worden geanalyseerd om de systemen te identificeren die kunnen worden geüpgraded naar de nieuwste versie van Windows.

U kunt ook een asset-inventarisatie verkrijgen via een WSMAN/WinRM-opdrachtregel of een CIM-clientopdrachtregel.

SCCM-integratie

U kunt SCCM met Dell Command | Monitor voor Windows integreren door:

- Het MOF-bestand in het installatiepakket van Dell Command | Monitor te gebruiken, dat alle Dell Command | Monitor klassen bevat, en het in ConfigMgr te importeren

Het MOF-bestand bevindt zich op:

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

- Assetrapportagemogelijkheden uitbreiden met behulp van verzamelingen

Scenario 2: Configuratiebeheer

Een bedrijf is van plan om het clientplatform te standaardiseren en elk systeem tijdens diens hele levenscyclus te beheren. Om deze inspanning te kunnen realiseren, schaft het bedrijf een set tools aan. Het plant het automatiseren van het gebruik van een nieuw clientbesturingssysteem met behulp van de Preboot Execution Environment (PXE).

Het probleem is het aanpassen van het BIOS-wachtwoord van elke clientcomputer zonder handmatig elk bureaublad te bezoeken. Als Dell Command | Monitor op elk clientsysteem is geïnstalleerd, heeft de IT-afdeling van het bedrijf meerdere opties om op afstand de

opstartvolgorde te wijzigen. De OpenManage Essentials (OME) is een beheerconsole die kan worden geïntegreerd met Dell Command | Monitor en die kan worden gebruikt voor het op afstand controleren van de BIOS-instellingen op alle clientsystemen. Een andere mogelijkheid is het schrijven van een script (CIM, WinRM/WSMAN/PowerShell/WMIC) dat de BIOS-instelling wijzigt. Het script kan op afstand worden aangeleverd via het netwerk en op elk clientsysteem worden uitgevoerd.

Voor meer informatie over Dell Command | Monitor raadpleegt u de Dell Command | Monitor naslaggids op dell.com/support.

Gestandaardiseerde configuraties kunnen aanzienlijke kostenbesparingen opleveren voor bedrijven van allerlei grootten. Veel organisaties implementeren gestandaardiseerde clientsystemen, maar weinige beheren de systeemconfiguratie gedurende de levensduur van de computer. Als Dell Command | Monitor op elk clientsysteem is geïnstalleerd, kan de IT-afdeling oudere poorten vergrendelen om het gebruik van niet-geautoriseerde randapparatuur te voorkomen of kan men WOL (Wake On LAN) inschakelen om het systeem buiten de piekuren uit een slaapstand te wekken om systeembeheertaken uit te voeren.

Scenario 3: Statuscontrole

Een gebruiker ontvangt leesfoutberichten tijdens een poging toegang te krijgen tot bepaalde bestanden op de harde schijf van het clientsysteem. De gebruiker start het systeem opnieuw op en de bestanden lijken nu toegankelijk te zijn. De gebruiker negeert het oorspronkelijke probleem omdat het lijkt alsof het vanzelf is opgelost. Ondertussen controleert Dell Command | Monitor de harde schijf met het probleem op een voorspellende fout en wordt een SMART-melding (Self-Monitoring, Analysis and Reporting Technology) doorgegeven aan de beheerconsole. Het programma geeft ook de SMART-foutmelding weer aan de lokale gebruiker. De melding geeft aan dat er meerdere lees- en schrijffouten optreden op de harde schijf. De IT-afdeling van het bedrijf adviseert de gebruiker onmiddellijk een back-up van belangrijke databestanden te maken. Er komt een servicetechnicus met een vervangende schijf.

De harde schijf wordt vervangen voordat deze kapot gaat, waardoor de gebruiker niet te maken krijgt met downtime, een gesprek met de helpdesk en een technicus die de desktop nakijkt om de oorzaak van het probleem vast te stellen.

Systemwaarschuwingen bewaken via Logboeken, Syslog of CIM-indicatie van het besturingssysteem

Dell Command | Monitor ondersteunt bewaking van gebeurtenissen via de volgende procedures:

- Het opvragen van het logboek via CIM-klasse DCIM_LogEntry.
- Het bewaken van CIM-indicatie via de klasse DCIM_AlertIndication.
- (Alleen voor Dell Command | Monitor voor Windows) gebeurtenissen bewaken via Simple Network Management Protocol (SNMP) en Windows-logboeken.
- (Alleen voor Dell Command | Monitor voor Linux) bewaken via Syslog.

Voor meer informatie over Dell Command | Monitor raadpleegt u de Dell Command | Monitor naslaggids op dell.com/support.

Scenario 4: Profielen

 **OPMERKING:** DMTF-profielen worden alleen voor Dell Command | Monitor voor Windows geïmplementeerd.

Er wordt van IT-beheerders verwacht dat ze clientsystemen beheren in omgevingen met meerdere leveranciers en gedistribueerde bedrijven. Ze worden geconfronteerd met uitdagingen omdat ze een reeks uiteenlopende tools en applicaties onder de knie moeten krijgen. Dat is nodig omdat ze meerdere desktop- en mobiele clientsystemen in verscheidene netwerken beheren. Om de kosten van deze vereisten te drukken en de beschikbare beheerdata weer te geven, zijn de industriestandaard DTMF- (Distributed Management Task Force) en DCIM OEM-profielen (Data Center Infrastructure Management) geïmplementeerd in Dell Command | Monitor. Een aantal van de DMTF-profielen wordt in deze handleiding beschreven.

Meer informatie over Dell Command | Monitor vindt u in de Dell Command | Monitor naslaggids op dell.com/support.

Assetprofiel

Garantiestatus op eindpuntapparaat:

- Bepaal de status van de garantie door de klasse **DCIM_AssetWarrantyInformation** te inventariseren of op te halen.
- Controleer of de garantiestatus kan worden bepaald met behulp van de eigenschappen **WarrantyStartDate** en **WarrantyEndDate** van de klasse **DCIM_AssetWarrantyInformation**.

OPMERKING: Vereiste voor DCIM_AssetWarrantyInformation is dat u een werkende internetverbinding hebt. Als u Dell Command | Monitor uitvoert achter een proxyserver, zorg dan dat de proxy-instellingen juist zijn geconfigureerd.

Voor meer informatie over de garantiestatus van de randapparatuur:

1. Ga naar Dell.com/support
 2. Selecteer uw land of regio in de vervolgkeuzelijst 'Kies een land/regio' onder aan de pagina
 3. Selecteer de support-categorie 'Garantie en contracten'
 4. Geef de juiste servicetag van uw systeem op
- Schakel de garantiefunctie en volgende vernieuwingsoproepen uit.
 - Vraag on-demand om garantie-informatie.

OPMERKING: De garantie-informatie wordt elke 15 dagen automatisch bijgewerkt. In het geval van een recente garantiestatus kan de weergegeven garantie-informatie afwijken van de op de Dell Support site weergegeven informatie.

Batterijprofiel

- Bepaal de status van de batterij door een instantie van de klasse **DCIM_Battery** te inventariseren of op te halen.
- Bepaal de geschatte werkingstijd en geef de geschatte resterende lading weer.
- Controleer of de statusinformatie voor de batterij kan worden vastgesteld met de eigenschappen Operational Status en HealthState van de klasse **DCIM_Battery**.
- Haal extra informatie op over de status van de batterij met de eigenschap **DCIM_Sensor.CurrentState** of de eigenschap **CIM_NumericSensor.CurrentState**.
- Bepaal de locatie van de batterij en de ePPID van de batterij met behulp van de eigenschappen **IdentifyingDescriptions** en **OtherIdentifyingInfo** van de klasse **DCIM_Battery**.

DCIM_Battery

Voor informatie over de ePPID-waarde van de batterij voor een batterij-element. Open een PowerShell-prompt met administratorbevoegdheden en voer de volgende opdracht uit `Get-CimInstance -Namespace root/dcim/sysman -Classname DCIM_Battery |Select ElementName, OtherIdentifyingInfo, IdentifyingDescriptions`.

OPMERKING: De ePPID-waarde van de batterij is niet dynamisch en als de batterij wordt vervangen, moet u het systeem opnieuw opstarten om de wijzigingen in de **DCIM_Battery**-instantie weer te geven.

Profiel BIOS-beheer

- Bepaal de BIOS-versie door de instantie van de klasse **DCIM_BIOSElement** te inventariseren.
- Controleer of de BIOS-kenmerkwaarden kunnen worden gewijzigd of niet. Haal de instantie van de klasse **DCIM_BIOSEnumeration** op. Het kenmerk kan worden gewijzigd als de eigenschap **IsReadOnly** is ingesteld op FALSE.
- Stel het systeemwachtwoord in (SystemPwd). Voer de methode **DCIM_BIOSService.SetBIOSAttributes()** uit en stel SystemPwd in op de parameter **AttributeName** en de wachtwoordwaarde op de parameter **AttributeValue**.
- Stel het BIOS- of Administrator-wachtwoord in (AdminPwd). Voer de methode **DCIM_BIOSService.SetBIOSAttributes()** uit en stel AdminPwd in op de parameter **AttributeName** en de wachtwoordwaarde op de parameter **AttributeValue**.
- Voer de methode **DCIM_BIOSService.SetBIOSAttributes()** uit en geef de parameters **AttributeName** en **AttributeValue** op.
- Als u een BIOS-kenmerk wilt wijzigen wanneer er een BIOS- of Admin-wachtwoord is ingesteld, voert u de methode **DCIM_BIOSService.SetBIOSAttributes()** uit en geeft u de **AttributeName** en **AttributeValue** op en geeft u het huidige BIOS-wachtwoord op als de **AuthorizationToken**-invoerparameter.

Opstartbeheer

- Verander de volgorde van de opstartitems in de Legacy- en UEFI-opstartlijst.
- Schakel de opstartitems in de Legacy en UEFI-opstartlijst in of uit.
- Zoek de huidige opstartconfiguratie op door de instanties van de klasse **DCIM_ElementSettingData** te inventariseren, waarvan de eigenschap **IsCurrent** op 1 is ingesteld. De **DCIM_BootConfigSetting** vertegenwoordigt de huidige opstartconfiguratie.

Mobiel basisbureaublad

- Bepaal het systeemmodel, de servicetag en het serienummer door de instantie van de klasse, **DCIM_ComputerSystem**, te inventariseren.
- U kunt de methode **DCIM_ComputerSystem.RequestStateChange()** uitvoeren om de waarde van de parameter RequestedState in te stellen op **3**. De parameterwaarde 3, schakelt het systeem uit.
- U kunt de methode **DCIM_ComputerSystem.RequestStateChange()** uitvoeren om de waarde van de parameter **RequestedState** in te stellen op **11**. De parameterwaarde 11, start het systeem opnieuw op.
- Bepaal de aan/uit-status van het systeem.
- Bepaal het aantal processors in het systeem door een query uit te voeren op **DCIM_Processor**, instanties die aan de Central Instance zijn gekoppeld via de koppeling **DCIM_SystemDevice**.
- Haal de systeemtijd op. Voer de methode **DCIM_TimeService.ManageTime()** uit en stel de parameter **GetRequest** in op **True**.
- Controleer de status van het beheerde element.

Logboekrecord

- Identificeer de logboeknaam door de **DCIM_RecordLog**-instantie te selecteren waarin de eigenschap **ElementName** met de logboeknaam overeenkomt.
- Zoek de afzonderlijke logboekvermeldingen. Haal alle instanties van **DCIM_LogEntry** op die zijn gekoppeld aan de opgegeven instantie van **DCIM_RecordLog** via de **DCIM_LogManagesRecord** koppeling. Sorteer de instanties op basis van de **RecordID**.
- Controleer of recordlogs zijn ingeschakeld door de instantie van de klasse **DCIM_RecordLog** te inventariseren waarvan de eigenschap **Enabledstate** is ingesteld op **2** (ingeschakeld) en waarvan **EnabledState** is ingesteld op **3** (uitgeschakeld).
- Sorteer de logboekrecords op basis van het tijdstempel van de logboekvermelding. Haal alle instanties van **DCIM_LogEntry** op die zijn gekoppeld aan de opgegeven instantie van **DCIM_RecordLog** via de **DCIM_LogManagesRecord** koppeling. Sorteer de instanties van **DCIM_LogEntry** op basis van de waarde van de eigenschap **CreationTimeStamp** in LIFO-volgorde (last in first out).
- Wis logboeken door de methode **ClearLog()** uit te voeren voor de gegeven instantie van het **DCIM_RecordLog**.

Fysieke asset

- Voer een fysieke inventarisatie uit voor alle apparaten in een systeem.
- Voer een fysieke inventarisatie uit voor een systeembehuizing.
- Bepaal het onderdeelnummer van een defect rakend onderdeel.
- Bepaal of een slot al dan niet leeg is.

Profiel systeemgeheugen

- Haal informatie op over het geheugen van het systeem.
- Haal informatie op over het fysieke geheugen van het systeem.
- Controleer de grootte van het systeemgeheugen.
- Controleer de grootte van het beschikbare systeemgeheugen.
- Controleer de grootte van het fysieke systeemgeheugen.
- Controleer de status van het systeemgeheugen.

Dell Command | Monitor 10.6 gebruiken

U kunt de door Dell Command | Monitor versochte informatie bekijken via: `root\dcim\sysman (standard)`

Dell Command | Monitor verstrekt de informatie via klassen in deze namespaces.

Meer informatie over de klassen, vindt u in de Dell Command | Monitor naslaggids op dell.com/support.

Onderwerpen:

- [Polling-interval instellen](#)
- [Statusrapportage RAID](#)
- [De Dell clientsystemen controleren](#)
- [Applicatielogboek voor Dell Command | Monitor voor Linux](#)
- [Stations met geavanceerde indeling detecteren](#)
- [Opstartconfiguraties](#)
- [De systeeminstellingen wijzigen](#)

Polling-interval instellen

U kunt met Dell Command | Monitor het polling-interval wijzigen van ventilatorsensor, temperatuursensor, spanningssensor, huidige sonde, toename/afname schijfcapaciteit, toename/afname geheugengrootte en toename/afname aantal processors.

- Voor Windows is het bestand `dcsbdy32.ini` of `dcsbdy64.ini` aanwezig in `<Dell Command | Monitor installed location>\omsa\ini`.
- Voor Linux is het bestand `AlertPollingSettings.ini` aanwezig in `/opt/dell/dcm/conf`.

OPMERKING: De getallen in het INI-bestand worden vermenigvuldigd met **23**. Het standaard polling-interval voor schijfcapaciteit en SMART-meldingen (Self-Monitoring Analysis and Reporting Technology) is **626** seconden (de echte tijd = 626 X 23 seconden, ongeveer 3 uur).

Statusrapportage RAID

Dell Command | Monitor schakelt de RAID-configuratiegegevens in en controleert de RAID-functionaliteit voor clientsystemen met hardware- en driverondersteuning. U kunt RAID-klassen gebruiken om de gegevens van RAID-niveaus, driverinformatie, controllerconfiguratie en controllerstatus te ontvangen. Nadat de RAID-configuratie is ingeschakeld, kunt u meldingen ontvangen voor de degradatie of fouten in schijven en controllers.

OPMERKING: RAID-statusrapportage wordt alleen ondersteund voor de RAID-controllers die werken met drivers die compatibel zijn met Common Storage Management Interface (CSMI) versie 0.81. OMCI 8.1 en latere versies ondersteunen het controleren alleen op de Intel on-chip RAID-controller; en OMCI 8.2 en latere versies ondersteunen de meldingsfunctie voor de Intel on-chip RAID-controller.

De Dell clientsystemen controleren

- Dell Command | Monitor Dell Command | Monitor voor Windows ondersteunt Simple Network Management Protocol (SNMP) voor het controleren en beheren van clientsystemen zoals notebooks, desktops en workstations. Het MIB-bestand (Management Information Base) wordt gedeeld tussen Dell Command | Monitor en Server Administrator. Dell Command | Monitor voor Windows is met ingang van versie 9.0 gewijzigd om een OID te gebruiken dat specifiek is voor de client-OID (10909), zodat consoles clientsystemen kunnen identificeren.

Meer informatie over SNMP vindt u in de Dell Command | Monitor SNMP-naslaggids op dell.com/support.

- Dell Command | Monitor voor Linux ondersteunt controleren met WinRM- en WSMAN-opdrachten.

Applicatielogboek voor Dell Command | Monitor voor Linux

Dell Command | Monitor voor Linux scheidt de applicatielogboeken en meldingen voor rapportage en foutopsporing. De geschiedenis van de gegenereerde meldingen en logboeken van de Dell Command | Monitor applicatie kan worden bekeken in het bestand **dcm_application.log** in `/opt/dell/dcm/var/log`.

Configuratiebestand

U kunt **log.property** van het configuratiebestand in `/opt/dell/dcm/conf` bijwerken om de gewenste instellingen en DEBUG toe te passen:

OPMERKING: Start de OMI-server opnieuw nadat u het configuratiebestand hebt gewijzigd om de wijzigingen toe te passen.

- **Log_Level:** er zijn drie logboekniveaus voor het scheiden van de systeemberichten: ERROR, INFO, DEBUG

De gebruiker kan het logboekniveau wijzigen via het configuratiebestand. Als het logboekniveau is ingesteld op DEBUG, stuurt de Dell Command | Monitor applicatie alle logboekinformatie naar het opgegeven logbestand.

OPMERKING: Het standaardlogboekniveau is ingesteld op INFO.

- **File_Size:** de gebruiker kan de maximale grootte van het bestand **dcm_application.log** opgeven. De standaard bestandsgrootte is 500 MB.

OPMERKING: De waarde **File_Size** moet worden uitgedrukt in bytes.

- **BackupIndex:** de gebruiker kan de rollover-telling van het bestand **dcm_application.log** opgeven. Als de standaard rollover-telling 2 is, zal het derde back-upbestand het oudste bestand negeren.

Stations met geavanceerde indeling detecteren

Clientsystemen gaan over naar AF-schijven (Advanced Format, geavanceerde indeling) voor een grotere storagecapaciteit en om de beperkingen van de harde schijven met sectoren van 512 bytes te elimineren. Systemen die overgaan naar schijven met sectoren van 4 KB, behouden achterwaartse compatibiliteit, terwijl de huidige AF-harde schijf, de 512e harde schijf, overeenkomt met 512-bytes SATA en werkt met 4 KB. Tijdens de transitie kunt u prestatieproblemen ondervinden, zoals defecte schijfstations in de clientsystemen die resulteren in fouten in sectorgebaseerde versleutelingssoftware die met 512e-schijven werken. Met Dell Command | Monitor kunt u bepalen of de harde schijf op een systeem een 4 KB AF-schijf is, wat helpt om zulke problemen te voorkomen.

Opstartconfiguraties

OPMERKING: Dell Command | Monitor voor Linux biedt geen mogelijkheden voor opstartconfiguratie. Dit gedeelte is dus niet van toepassing op Dell Command | Monitor voor Linux.

Een client-systeem kan een van twee typen opstartconfiguratie hebben:

- Legacy (BIOS)
- UEFI

De opstartconfiguratie (Legacy of UEFI) wordt in Dell Command | Monitor gemodelleerd met behulp van de volgende klassen:

- DCIM_ElementSettingData
- DCIM_BootConfigSetting
- DCIM_OrderedComponent
- DCIM_BootSourceSetting
- DCIM_SmartAttributeInfo

OPMERKING: De termen Opstartconfiguratie en Opstartlijsttype worden door elkaar gebruikt en geven dezelfde betekenis aan met betrekking tot Legacy of UEFI.

DCIM_AssetWarrantyInformation

- Voer de volgende opdracht uit in de PowerShell-prompt om de garantiestatus op het eindpuntapparaat op te vragen:

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

- Voer de volgende opdracht uit in de PowerShell-prompt om de garantierechten van `WarrantyEndDate` in chronologische volgorde weer te geven:

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

- Voer de volgende opdracht uit in de PowerShell-prompt om de garantiefunctie en de daaropvolgende vernieuwingsoproepen uit te schakelen:

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

- Om garantie-informatie on-demand op te halen, voert u de volgende opdracht uit in de PowerShell-prompt:

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

OPMERKING: Instelling voor proxyconfiguratie -

- Standaardproxy – Dell Command | Monitor selecteert de standaard systeempoxy (ingesteld in IE)
- Aangepaste proxy

DCIM_ApplicationProxySetting-klasse wordt gebruikt om de proxy-instellingen voor Dell Command | Monitor aan te passen aan de proxy-omgeving.

DCIM_BootConfigSetting

Een instantie van **DCIM_BootConfigSetting** vertegenwoordigt een opstartconfiguratie die wordt gebruikt tijdens het opstartproces. Op clientsystemen zijn er bijvoorbeeld twee soorten opstartconfiguraties — Legacy en UEFI. **DCIM_BootConfigSetting** kan dus maximaal twee instanties bevatten, één voor Legacy en één voor UEFI.

U kunt bepalen of **DCIM_BootConfigSetting** Legacy vertegenwoordigt, waarbij de volgende eigenschappen worden gebruikt:

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

U kunt bepalen of de **DCIM_BootConfigSetting** UEFI vertegenwoordigt, waarbij de volgende eigenschappen worden gebruikt:

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

DCIM_BootSourceSetting

Deze klasse vertegenwoordigt de opstartapparaten of bronnen. De eigenschappen **ElementName**, **BIOSBootString** en **StructuredBootString** bevatten een tekenreeks die de opstartapparaten identificeert. Bijvoorbeeld: diskette, harde schijf, cd/dvd, netwerk, PCMCIA-kaart, Battery Electric Vehicle (BEV) of USB. Op basis van het type opstartlijst van het apparaat, wordt een instantie van **DCIM_BootSourceSetting** gekoppeld aan een van de instanties van **DCIM_BootConfigSetting**.

DCIM_OrderedComponent

De koppelingsklasse **DCIM_OrderedComponent** wordt gebruikt om instanties van **DCIM_BootConfigSetting** te koppelen aan instanties van **DCIM_BootSourceSetting** die een van de opstartlijsttypen (Legacy of UEFI) vertegenwoordigen waartoe de opstartapparaten behoren. De eigenschap **GroupComponent** van **DCIM_OrderedComponent** verwijst naar de instantie **DCIM_BootConfigSetting** en de eigenschap **PartComponent** verwijst naar de instantie **DCIM_BootSourceSetting**.

DCIM_Smart kenmerk

Voor het lezen van de smart kenmerkwaarde voert u de volgende opdrachten uit:

Bijvoorbeeld:

- `Get-CimInstance -Namespace root\dcim\sysman DCIM_SmartAttributeInfo | Format-Table`
- `Get-CimInstance -Namespace root\DCIM\sysman DCIM_SmartAttributeInfo -Filter "AttributeID zoals '< Kenmerk ID waarde >'"`

Voor het instellen van de aangepaste drempelwaarden voert u de volgende opdrachten uit:

Bijvoorbeeld:

- `Get-CimInstance -Namespace root\DCIM\sysman DCIM_SmartAttributeInfo -Filter "AttributeID zoals '<Kenmerk ID Waarde>'" | Invoke-CimMethod -MethodName "SetCustomThreshold" -Argumenten @{CustomThresholdValue="<aangepaste drempelwaarde moet worden ingesteld>"}`

DCIM_ThermalInformation

DCIM_ThermalInformation beheert thermische configuratie-instellingen zoals Thermische modus, AAC-modus en Ventilatorstoringmodus.

- Voer de volgende opdracht uit om de thermische informatie over het apparaat op de vragen:


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

- Voer de volgende opdracht uit om de waarde van de thermische modus in te stellen:

```
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"}
```

De systeeminstellingen wijzigen

In Dell Command | Monitor gebruikt u de volgende methoden voor het wijzigen van de systeeminstellingen en status van de lokale of externe systemen:

- `SetBIOSAttributes` - voor het wijzigen van de BIOS-instelling
-  **OPMERKING:** Dell Command | Monitor voor Linux ondersteunt momenteel alleen de `SetBIOSAttributes`-methode.
- `ChangeBootOrder` - voor het wijzigen van de opstartconfiguratie
 - `RequestStateChange` - voor het afsluiten en het opnieuw opstarten van het systeem
 - `ManageTime` - voor het weergeven van de systeemtijd

In Dell Command | Monitor voor Windows kunt u deze methoden uitvoeren met `wirm`, `VBscript`, `PowerShell`-opdrachten, `wmic` en `WMI` `wbentest`.

Het BIOS opnieuw instellen op de standaardinstellingen voor Windows- of Linux-systemen

`ResetBIOSDefaults` (methode)

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

OMI-opdracht: `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> }`

Mogelijke waarden:

- 0-Geïntegreerde veilige standaardwaarden: Dit staat bekend als de BIOS-standaardinstellingen. Deze configuratie ondersteunt alle platformen en daarom kan de configuratie niet worden gewijzigd.

- 1- Laatste bekende goede configuratie: Deze wordt automatisch gegenereerd door het BIOS nadat de POST is voltooid. Met deze optie wordt het BIOS teruggezet naar een goede configuratie. Als de **Geïntegreerde veilige standaardwaarden** beschadigd zijn, kunt u **Laatste bekende goede configuratie** gebruiken om het BIOS te herstellen.
- 2-Fabrieksinstellingen: Fabrieksinstellingen worden gegenereerd voordat het systeem wordt verzonden. Deze configuratie is geoptimaliseerd voor de hardwareconfiguratie of wordt aangepast aan uw vereisten tijdens de aankoop of service.
- 3-Gebruikersconfiguratie 1: Deze wordt geconfigureerd wanneer de gebruiker dit nodig heeft. U moet **Huidige configuratie opslaan** kiezen in de BIOS-instellingen of het F2-scherf om de configuratie opnieuw in te stellen via de applicatie Dell Command | Monitor.
- 4-Gebruikersconfiguratie 2: Deze wordt geconfigureerd wanneer de gebruiker dit nodig heeft. U moet **Huidige configuratie opslaan** kiezen in de BIOS-instellingen of het F2-scherf om de configuratie opnieuw in te stellen via de applicatie Dell Command | Monitor.

Tabel 1. Mogelijke waarden van ResetBIOSDefaults

Beschrijving	Foutcode (SetResult-waarde)
Geslaagd	0
Ongeldige invoerwaarde/invoerwaarde buiten bereik	1
Authenticatiefout	2
Niet-ondersteunde configuratie	3
Lege configuratie	4
Generieke fout/mislukt/wanneer de service niet wordt uitgevoerd	4294967295

OPMERKING: Na de bewerking **ResetBIOSDefaults** moet het systeem opnieuw worden opgestart om de wijzigingen toe te passen.

DCM-vensters beschikken over de functionaliteit om het systeem uit te schakelen of opnieuw op te starten via de volgende API's:

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

De volgende API's kunnen worden gebruikt in het GNU- of Linux-besturingssysteem:

- shutdown -r +5
- sudo reboot

OPMERKING: Tijdens de reset-bewerking wordt een subset van opties niet teruggezet op de standaardwaarden. Dit kan zijn vanwege veiligheidsredenen (bijvoorbeeld wachtwoorden) of de mogelijkheid om op te starten (bijvoorbeeld opstartlijst en Legacy Option-ROM's).

De BIOS-gebeurtenislogboeken worden niet gereset om de geschiedenis van de systeemhardware op te slaan.

De volgende tabel bevat de uitgebreide lijst met functies die niet naar de standaardwaarden worden teruggezet.

Tabel 2. Uitgebreide lijst met functies die niet naar de standaardwaarden worden teruggezet

Sectie	Subsectie	Onderdeel
Algemeen	Systeeminformatie	Servicetag
	Systeeminformatie	Asset-tag
	Systeeminformatie	Eigendomstag
	Opstartvolgorde	Opstartlijst
	Geavanceerde opstartopties	Legacy OROM's inschakelen
	Datum/Tijd	Datum/Tijd
	Geïntegreerde NIC	Geïntegreerde NIC
	Geïntegreerde NIC	UEFI-netwerkstack inschakelen
	SATA-bediening	SATA-bediening

Tabel 2. Uitgebreide lijst met functies die niet naar de standaardwaarden worden teruggezet (vervolg)

Sectie	Subsectie	Onderdeel
Beveiliging	N.v.t.	Administrator-wachtwoord
	N.v.t.	Systeemwachtwoord
	N.v.t.	Interne HDD-x wachtwoord(en)
	N.v.t.	Uitsluiting hoofdwachtwoord
	SMM-beveiligingsbeperking	SMM-beveiligingsbeperking
	Intel SGX inschakelen	Intel SGX inschakelen
Veilig opstarten	Veilig opstarten inschakelen	Veilig opstarten inschakelen
	Geavanceerd sleutelbeheer	Sleuteldatabases

BIOS-kenmerken in een Windows-systeem instellen met behulp van PowerShell-opdrachten

U kunt BIOS-kenmerken instellen met behulp van de SetBIOSAttributes-methode. De procedure wordt hieronder uitgelegd aan de hand van het inschakelen van de Trusted Platform Module (TPM) als voorbeeld.

OPMERKING: Zorg ervoor dat de TPM-optie is uitgeschakeld in het BIOS voordat u de procedure voor het inschakelen van de TPM volgt.

OPMERKING: Gebruik PowerShell met administratorbevoegdheden.

TPM inschakelen:

- Als er nog geen BIOS-wachtwoord op het systeem is ingesteld, dient u dit in te stellen met de volgende PowerShell-opdracht:

```
Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSService
| Invoke-CimMethod -MethodName SetBIOSAttributes -Arguments
@{AttributeName=@("AdminPwd");AttributeValue=@("<Admin password>") }
```

- Schakel TPM-beveiliging in met de volgende opdracht:

```
Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSService | Invoke-CimMethod
-MethodName SetBIOSAttributes -Arguments @{AttributeName=@("Trusted Platform Module
");AttributeValue=@("1");AuthorizationToken="<Admin password>"} 
```

- Start het systeem opnieuw op.

- Activeer de TPM met de volgende opdracht:

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

- Start het systeem opnieuw op.

Algemene afwijzing van aansprakelijkheid

Met de PowerShell PSReadline-module wordt elke consoleopdracht die u invoert in een tekstbestand opgeslagen. Het wordt daarom ten zeerste aanbevolen om de commandlet 'Get-Credential' te gebruiken om het wachtwoord veilig te verwerken.

- \$cred = Get-Credential
- Voer uw gebruikersnaam en wachtwoord in, bijvoorbeeld AdminPWD en Dell_123\$, wanneer het dialoogvenster wordt weergegeven.
- \$BSTR = [System.Runtime.InteropServices.Marshal]::SecureStringToBSTR(\$cred.Password)
- \$plainpwd=[System.Runtime.InteropServices.Marshal]::PtrToStringAuto(\$BSTR)
- Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSService | Invoke-CimMethod MethodName SetBIOSAttributes -Arguments @{AttributeName=@("AdminPwd");AttributeValue=@("\$plainpwd ")}

BIOS-kenmerken instellen in het Linux-systeem


U kunt BIOS-kenmerken instellen via de volgende methoden:

- [OMICLI gebruiken](#)
- [WinRM gebruiken](#)
- [WSMan gebruiken](#)

 **OPMERKING:** Zorg dat de OMI-server is gestart en actief is.

BIOS-kenmerken instellen met OMICLI

U kunt BIOS-kenmerken instellen met behulp van de SetBIOSAttributes-methode. De procedure wordt hieronder uitgelegd aan de hand van het inschakelen van de Trusted Platform Module (TPM) als voorbeeld.

 **OPMERKING:** Zorg ervoor dat de TPM-optie is uitgeschakeld in het BIOS voordat u de procedure voor het inschakelen van de TPM volgt.

BIOS-kenmerken instellen met OMICLI-opdrachten:

1. Als u het BIOS-wachtwoord op het systeem wilt instellen als dit nog niet is ingesteld, voert u uit:

```
./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. Als u TPM-beveiliging wilt inschakelen met de volgende opdracht, voert u uit:

```
./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. Start het systeem opnieuw op.
4. Om de TPM te activeren, voert u uit:


```
./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. Start het systeem opnieuw op.
6. Om het BIOS-wachtwoord opnieuw in te stellen, voert u uit:

```
./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>" }
```

BIOS-kenmerken instellen met WinRM

U kunt BIOS-kenmerken instellen met behulp van de SetBIOSAttributes-methode. De procedure wordt hieronder uitgelegd aan de hand van het inschakelen van de Trusted Platform Module (TPM) als voorbeeld.

 **OPMERKING:** Zorg dat de TPM-optie is uitgeschakeld in het BIOS voordat u de procedure voor het inschakelen van de TPM volgt.

BIOS-kenmerken instellen met WinRM-opdrachten:

1. Haal de selectorset op door de DCIM_BIOSService-klasse te inventariseren. Uitvoeren:

```
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
```

OPMERKING: In dit voorbeeld worden de selectorsetwaarden (SystemName=<stelselnaam van DCIM_BIOSService-klasse>winrm i SetBIOSAttributes wsman/DCIM_BIOSService?SystemName=dt:+SystemCreationClassName=DCIM_ComputerSystem+Name=DCIM:BiosService+CreationClassName=DCIM_BIOSService+) voor het instellen gebruikt.

2. Als het BIOS-wachtwoord voor het systeem nog niet is ingesteld, kunt u dit doen met de volgende opdracht:

```
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. Schakel TPM-beveiliging in door de volgende opdracht uit te voeren:

```
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. Start het systeem opnieuw op.
5. Activeer de TPM met de volgende opdracht:

```
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>"}
```

BIOS-kenmerken instellen met WSMAN

U kunt BIOS-kenmerken instellen op de Linux-systemen met behulp van WSMAN. De procedure wordt hieronder uitgelegd aan de hand van het inschakelen van de Trusted Platform Module (TPM) als voorbeeld.

OPMERKING: Zorg dat de TPM-optie is uitgeschakeld in het BIOS voordat u de procedure voor het inschakelen van de TPM volgt.

1. Haal de selectorset op door de DCIM_BIOSService-klasse te inventariseren. Uitvoeren:

```
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. Als het BIOS-wachtwoord voor het systeem nog niet is ingesteld, kunt u dit doen met de volgende opdracht:

```
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. Schakel TPM-beveiliging in met de volgende opdracht:

```
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. Start het systeem opnieuw op.
5. Activeer de TPM met de volgende opdracht:

```
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>"
```

De opstartvolgorde wijzigen

Gebruik deze stappen om de opstartvolgorde te wijzigen:

1. Controleer het type opstartvolgorde (Legacy of UEFI) met de volgende opdracht:
 - WMIC-opdracht: `wmic /namespace:\\root\dcim\sysman path dcim_BootConfigSetting get ElementName/ format:list.`
 - PowerShell-opdracht: `Get-WmiObject -namespace root\dcim\sysman -class dcim_BootConfigSetting -Property ElementName.`
2. Controleer het huidige type opstartvolgorde (Legacy of UEFI) met de volgende opdracht:
 - WMIC-opdracht: `wmic /namespace:\\root\dcim\sysman path dcim_ElementSettingData.IsCurrent=1 get SettingData /format:list .`
 - PowerShell-opdracht: `Get-WmiObject -namespace root\dcim\sysman -class dcim_elementSettingData -Filter "IsCurrent=1" -Property SettingData.`
3. De opstartvolgorde wijzigen met de volgende opdracht:
 - WMIC-opdracht: `wmic /namespace:\\root\dcim\sysman path dcim_bootconfigsetting call ChangeBootOrder /?:full .`
 - PowerShell-opdracht: `(Get-WmiObject -namespace root\dcim\sysman -class dcim_bootconfigsetting).getmethodparameters("ChangeBootOrder") .`
 -  **OPMERKING:** De instantie `dcim_BootConfigSetting` moet de opstartconfiguratie zijn die u wilt wijzigen – type 1 (Legacy) of type 2 (UEFI).
 - De argumenten zijn:
 - `Authorization Token` — Dit is het administratorwachtwoord of opstartwachtwoord.
 - `Source` — Dit is de opstartvolgordelijst die is overgenomen uit de eigenschap `dcim_OrderedComponent.PartComponent`. De nieuwe opstartvolgorde wordt bepaald door de volgorde van de opstartapparaten in de bronarray.
4. De opstartvolgorde van type 1-opstartlijst wijzigen met behulp PowerShell:
 - a. Haal de huidige opstartvolgorde van de type 1-opstartlijst op met de volgende opdracht: `$boLegacy = Get-WmiObject -namespace root\dcim\sysman -class dcim_orderedcomponent | where {$_.partcomponent -match 'BootListType-1'} | select -expand partcomponent.`
 - b. Definieer een PowerShell-variabele om de opstartvolgorde op te geven voor het instellen van `$newboLegacy`. Wijs er de nieuwe opstartvolgorde aan toe. Bijvoorbeeld: het huidige type opstartvolgorde blijft behouden.
 - c. `$newboLegacy = $boLegacy`
 - d. Haal de `dcim_bootconfigsetting`-instantie op die overeenkomt met de type 1-opstartlijst met de volgende opdracht: `$bcsLegacy = Get-WmiObject -Namespace root\dcim\sysman -ClassName dcim_bootconfigsetting | where {$_.ElementName -eq 'Next Boot Configuration Setting : Boot List Type 1'}.`

- e. Roep de methode aan met de volgende opdracht: `$ bcsLegacy.changebootorder ($newboLegacy, $AuthorizationToken)`. De variabele `$AuthorizationToken` wordt gebruikt voor het doorgeven van het BIOS-wachtwoord.
5. De opstartvolgorde van type 2-opstartlijst wijzigen met behulp PowerShell:
- a. Haal de huidige opstartvolgorde van de type 2-opstartlijst op met de volgende opdracht: `$boUefi = Get-WmiObject -namespace root\dcim\sysman -class dcim_orderedcomponent | where {$_.partcomponent -match 'BootListType-2'} | select -expand partcomponent`.
 - b. Definieer een PowerShell-variabele om de opstartvolgorde op te geven voor het instellen van `$newboUefi`. Wijs er de nieuwe opstartvolgorde aan toe. Bijvoorbeeld: het huidige type opstartvolgorde blijft behouden.
 - c. Haal de `dcim_bootconfigsetting` instantie op die overeenkomt met de type 2-opstartlijst met de volgende opdracht: `$bcsUefi = Get-WmiObject -Namespace root\dcim\sysman -ClassName dcim_bootconfigsetting | where {$_.ElementName -eq 'Next Boot Configuration Setting : Boot List Type 2'}`.
 - d. Roep de methode aan met de volgende opdracht: `$ bcsUefi.changebootorder ($newboUefi, $AuthorizationToken)`. De variabele `$AuthorizationToken` wordt gebruikt voor het doorgeven van het BIOS-wachtwoord.

Het Windows-systeem op afstand afsluiten en opnieuw opstarten

U kunt het Windows-systeem op afstand afsluiten of opnieuw opstarten met behulp van de `RequestStateChange`-methode.

1. Schakel het Windows-systeem op afstand uit met behulp van de volgende opdracht:

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

2. Start het Windows-systeem op afstand opnieuw op met de volgende opdracht:

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

De systeemtijdwaarde voor een Windows-systeem op afstand ophalen

U kunt de systeemtijdwaarde voor het Windows-systeem op afstand verkrijgen met behulp van de `ManageTime`-methode. Bijvoorbeeld:

Voer in de opdrachtregelinterface het volgende uit:

- 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"}`

Het lokale beheer van Dell clientsystemen via Dell Command | Monitor 10.6

U kunt Dell clientsystemen lokaal aan de hand van de volgende methoden beheren:

- Voor systemen met Windows [via PowerShell](#)
- Voor systemen met Linux [via OMICLI](#)

Onderwerpen:

- [Windows-systemen lokaal beheren met PowerShell](#)
- [Linux-systemen lokaal beheren met OMICLI](#)

Windows-systemen lokaal beheren met PowerShell

Met behulp van PowerShell-opdrachten kunt u Dell clientsystemen met Windows lokaal beheren.

- Instanties van de DCIM-klasse specificeren
 - `Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSEnumeration`
 - `Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSPassword`
- Eigenschappen voor een BIOS-instelling ophalen

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

- BIOS-instellingen wijzigen

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

- Niet-kritieke waarden wijzigen

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

- Abonneren op waarschuwingen


```
$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)
```

- Opdrachten voor het ophalen van gebruikerstoestemming via WMI:

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

- Opdrachten voor het instellen van gebruikerstoestemming via WMI:

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

 **OPMERKING:** Het verbeteringsprogramma is beschikbaar voor Dell Command | Monitor 10.5 en 10.6 x64-bits versie.

- Opdrachten voor het ophalen van proxy via WMI:

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

- Opdrachten voor het instellen van proxy via WMI:

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

Linux-systemen lokaal beheren met OMICLI

U kunt Linux-systemen lokaal beheren met behulp van OMICLI-opdrachten. Op de systemen waarop Linux wordt uitgevoerd, is OMICLI geïnstalleerd in /opt/omi/bin.

- Instanties van de DCIM-klasse specificeren
 - ./omicli ei root/dcim/sysman DCIM_BIOSEnumeration
 - ./omicli ei root/dcim/sysman DCIM_BIOSPassword
- Eigenschappen voor een BIOS-instelling ophalen

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

- Administrator-wachtwoord instellen

```
./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 }
```

- BIOS-instellingen wijzigen

- ./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> }
```

- Abonneren op waarschuwingen

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

Het beheer van Dell clientsystemen op afstand met behulp van Dell Command | Monitor 10.6

U kunt Dell clientsystemen aan de hand van de volgende methoden op afstand beheren:

- Voor systemen met Windows, [Windows-systeem op afstand beheren met PowerShell](#) op pagina 25
- Voor systemen met Linux, [Linux-systeem beheren op afstand met Windows-systeem met WinRM](#) op pagina 25

Onderwerpen:

- [Windows-systeem op afstand beheren met PowerShell](#)
- [Linux-systeem beheren op afstand met Windows-systeem met WinRM](#)
- [Linux-systeem op afstand beheren via een Linux-systeem met WSMAN](#)

Windows-systeem op afstand beheren met PowerShell

U kunt een Windows-systeem op afstand openen en controleren via PowerShell.

Vereisten voor het beherende Windows-systeem:

- Windows PowerShell 3.0
- PowerShell moet zijn geconfigureerd voor het uitvoeren van externe scripts

Vereisten voor het beheerde Windows-systeem:

- Dell Command | Monitor
- Windows PowerShell 3.0
- PowerShell moet zijn geconfigureerd voor het uitvoeren van externe scripts
- De functie PowerShell-remoting moet zijn ingeschakeld

OPMERKING:

Om Windows PowerShell op afstand te gebruiken, moet de externe computer worden geconfigureerd voor beheer op afstand. Voor meer informatie, inclusief instructies, voert u de PowerShell-opdracht - `Get-Help about_remote_requirements` uit.

Linux-systeem beheren op afstand met Windows-systeem met WinRM

Met behulp van WinRM-opdrachten kunt u het systeem waarop Linux wordt uitgevoerd, benaderen en bewaken via het systeem waarop Windows wordt uitgevoerd.

Vereisten voor het Windows-systeem

- Ondersteund Windows-besturingssysteem
- WinRM-services die worden uitgevoerd en zijn geconfigureerd voor extern beheer

Vereisten voor het Linux-systeem

- Hoofdmapprivileges
- Dell Command | Monitor
- Ondersteund Linux-besturingssysteem
- Ingeschakelde poort 5985 en 5986 op de WMI-server
- Systeem is geconfigureerd voor uw omgeving

Voer uit in de opdrachtregelinterface

```
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
```

Linux-systeem op afstand beheren via een Linux-systeem met WSMAN

U kunt het systeem waarop Linux wordt uitgevoerd, op afstand benaderen en controleren via een Linux-systeem met behulp van WSMAN-opdrachten.

Vereisten voor het beherende Linux-systeem:

- Ondersteund Linux-besturingssysteempakket is geïnstalleerd
- wsmancli-pakket is geïnstalleerd

Vereisten voor het beheerde Linux-systeem:

- Hoofdmapprivileges
- Ondersteund Linux-besturingssysteem
- Dell Command | Monitor

Start een Terminal en voer uit:

```
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
```

Veelgestelde vragen over Dell Command | Monitor 10.6

- Hoe vind ik de opstartvolgorde van de opstartconfiguratie met de eigenschap `DCIM_OrderedComponent.AssignedSequence`?

Wanneer aan een **DCIM_BootConfigSetting**-instantie (Legacy of UEFI) meerdere **DCIM_BootSourceSetting**-instanties (opstartapparaten) zijn gekoppeld via instanties van de **DCIM_OrderedComponent**-koppeling, wordt de waarde van de eigenschap **DCIM_OrderedComponent.AssignedSequence** gebruikt om de volgorde te bepalen waarin de bijbehorende **DCIM_BootSourceSetting**-instanties (opstartapparaten) tijdens het opstartproces worden gebruikt. Een **DCIM_BootSourceSetting** waarvan de bijbehorende eigenschap **CIM_OrderedComponent.AssignedSequence** gelijk is aan **0**, wordt genegeerd en wordt niet als onderdeel van de opstartvolgorde beschouwd.

- Hoe kan ik de opstartvolgorde wijzigen?

De opstartvolgorde kan worden gewijzigd met de **DCIM_BootConfigSetting.ChangeBootOrder()** methode. De **ChangeBootOrder()** methode stelt de volgorde in waarin de instanties van **DCIM_BootSourceSetting** worden geassocieerd met een **DCIM_BootConfigSetting**-instantie. De methode heeft één invoerparameter: **Source**. De **Source**-parameter is een geordende array van het **PartComponent** eigendom van **DCIM_OrderedComponent**-klasse die de koppeling vertegenwoordigt tussen **DCIM_BootSourceSetting**-instanties (opstartapparaten) en de **DCIM_BootConfigSetting**-instantie (opstartlijsttype Legacy of UEFI).

- Hoe kan ik opstartapparaten uitschakelen?

Bij het wijzigen van de opstartvolgorde, wordt de waarde van de eigenschap **AssignedSequence** voor elke instantie van **DCIM_OrderedComponent**, die de doel-**DCIM_BootConfigSetting**-instantie koppelt aan een **DCIM_BootSourceSetting**-instantie die niet aanwezig is in de invoerarray van de parameter **Source**, op **0** ingesteld, wat aangeeft dat het apparaat uitgeschakeld is.

- Het bericht dat aanmelden is mislukt wordt weergegeven wanneer <wat verbinding probeert te maken> probeert verbinding te maken met de namespace met `wbemtest`.

Open **wbemtest** met administratorbevoegdheden om eventuele loginmeldingen te omzeilen. Ga naar Internet Explorer vanuit de lijst **Alle Programma's**, klik met de rechtermuisknop en selecteer **Als administrator uitvoeren** om de **wbemtest** te starten en een namespace-fout te voorkomen.

- Hoe kan ik Knowledge Library scripts probleemloos uitvoeren?

Hieronder staan de stappen voor het uitvoeren van de VBS-scripts die beschikbaar zijn in de Dell Command | Monitor Knowledge Library-koppeling:

1. Configureer **winrm** op het systeem waarop u de opdracht `winrm quickconfig` gebruikt.
2. Controleer of tokenondersteuning in het systeem aanwezig is. Raadpleeg hiervoor:
 - Het **F2-scherm** in BIOS Setup.
 - Gebruik een tool zoals `wbemtest`, waarmee u controleert of de sleutelwaarden die in het script zijn gedefinieerd, op het systeem voorkomen.

OPMERKING: Dell beveelt het gebruik aan van de nieuwste BIOS die beschikbaar is op dell.com/support. Voor meer informatie raadpleegt u de Dell Command | Monitor naslaggids op dell.com/support.

- Hoe stel ik de BIOS-kenmerken in?

BIOS-kenmerken kunnen worden gewijzigd met de **DCIM_BIOSService.SetBIOSAttributes()**-methode. De **SetBIOSAttributes()**-methode stelt de waarde in van de instantie die in de **DCIM_BIOSEnumeration**-klasse is gedefinieerd. De methode heeft zeven invoerparameters. De eerste twee parameters kunnen leeg of nul zijn. De derde parameter **AttributeName** moet de invoertoewijzing aannemen van de waarde van de kenmerknaam-instantie van de **DCIM_BIOSEnumeration**-klasse. De vierde parameter of **AttributeValue** kan een van de mogelijke waarden van de kenmerknaam zijn zoals gedefinieerd in de **DCIM_BIOSEnumeration**-klasse. De vijfde parameter `AuthorizationToken` is optioneel, de invoer voor vijfde parameter is een BIOS-wachtwoord. De vijfde parameter wordt alleen gebruikt wanneer het BIOS-wachtwoord op het systeem is ingesteld; anders is deze leeg. Het zesde en het zevende argument kunnen opnieuw leeg of nul zijn.

- Ondersteunt Dell Command | Monitor storage- en sensorcontrole voor Windows- en Linux-besturingssystemen?

Ja, Dell Command | Monitor ondersteunt zowel storage- als sensorcontrole voor ondersteunde Windows- en Linux-besturingssystemen.

Bij storagecontrole ondersteunt Dell Command | Monitor de controle van en waarschuwingen voor:

- o Met Intel geïntegreerde controller (compatibel met CSMI v0.81 of hoger)
- o Met LSI geïntegreerde RAID-controllers; en 9217, 9271, 9341, 9361 en de bijbehorende drivers (fysiek en logisch)

OPMERKING: Bewaking van met Intel geïntegreerde controller wordt niet ondersteund voor de systemen met Linux als besturingssysteem.

Bij sensorcontrole ondersteunt Dell Command | Monitor de controle van en waarschuwingen voor spannings-, temperatuur-, stroomsterkte-, koeling- (ventilator) en chassissensoren.

Zie de Dell Command | Monitor naslaggids op dell.com/support voor meer informatie over klassen en meldingen.

- Kan Dell Command | Monitor met andere applicaties/consols worden geïntegreerd?

Ja, Dell Command | Monitor kan worden geïntegreerd met toonaangevende bedrijfsbeheerconsols die de geldende normen voor de industrie ondersteunen. Het kan worden geïntegreerd met de volgende bestaande bedrijfsbeheersapplicaties:

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

- Kan ik klassen in SCCM importeren voor inventarisatie?

Ja, individuele MOF's of OMCI_SMS_DEF.mof-bestanden kunnen voor inventarisatie in SCCM-console worden geïmporteerd.

- Waar bevindt zich het SCCM-bestand OMCI_SMS_DEF.mof?

Het bestand OMCI_SMS_DEF.mof bevindt zich in C:\Program Files\Dell\Command_Monitor\ssa\omacim\OMCI_SMS_DEF.mof.

- De proxy voor DCM 10.2.1 configureren
- DCM 10.2.1 kan geen garantie-informatie ophalen.
- Controleer of de proxy-instellingen van de applicatie correct zijn geconfigureerd met behulp van de DCIM_ApplicationProxySetting-klasse.

Proxyreferenties configureren voor Dell Command | Monitor.

Als u zich hebt aangemeld via Dell Command | Monitor kunt u dezelfde referenties gebruiken voor proxyauthenticatie.

- Dell Command | Monitor geeft de garantie-informatie niet weer.

- o Het clientsysteem is niet verbonden met internet tijdens het navragen.

Maak verbinding met het internet en haal de garantie-informatie op door de volgende opdracht uit te voeren:

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

- o Het clientsysteem is niet geconfigureerd met de proxyserver.

Proxy-instellingen configureren in Dell Command | Monitor door de volgende opdrachten uit te voeren:

- Voer de volgende opdracht uit om de proxy op te halen uit de WMI: `Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_ApplicationProxySetting.`
- Voer de volgende opdracht uit om de proxy in te stellen vanuit de WMI: `Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_ApplicationProxySetting | Invoke-CimMethod -MethodName Change ProxySetting -Arguments @{NewAddress="10.0.0.223"; NewPort="8080"}`

U moet **NewAddress** en **NewPort** vervangen overeenkomstig de proxy-omgeving (indien van toepassing).

Stappen voor probleemoplossing met behulp van Dell Command | Monitor 10.6

Onderwerpen:

- Kan geen externe verbinding maken met Windows Management Instrumentation
- Installatiefout op systemen waarop Windows wordt uitgevoerd
- Inventarisatiewaarde van BIOS-instelling wordt weergegeven als 1
- Hapi-installatie mislukt vanwege de afhankelijkheid van libsmbios
- CIM-resource niet beschikbaar
- Kan opdrachten niet uitvoeren met behulp van DCM op de systemen met Ubuntu Core 16

Kan geen externe verbinding maken met Windows Management Instrumentation

Als CIM-informatie (Common Information Model) voor een extern clientcomputersysteem niet beschikbaar is voor de beheerapplicatie of als een externe BIOS-update waarvoor DCOM (Distributed Component Object Model) wordt gebruikt, mislukt, worden de volgende foutberichten weergegeven:

- **Toegang geweigerd**
- **Win32:RPC-server is niet beschikbaar**

1. Controleer of het clientsysteem is verbonden met het netwerk. Typ het volgende in de opdrachtrompt van de server:
ping <Host Name or IP Address> en druk op <Enter>.
2. Voer de volgende stap uit als zowel de server als het clientsysteem zich in hetzelfde domein bevinden:

- Controleer of de Administrator-account van het domein voor beide systemen administratorbevoegdheden heeft .

Voer de volgende stap uit als zowel de server als het clientsysteem zich in een werkgroep bevinden (niet in hetzelfde domein):

- Zorg dat de laatste Windows Server-versie wordt uitgevoerd op de server.

OPMERKING: Maak een back-up van uw systeemdatabestanden voordat u het register wijzigt. Als u het register onjuist bewerkt, kan uw besturingssysteem onbruikbaar worden.

3. Bewerk de registerwijziging op het clientsysteem. Klik op **Start > Uitvoeren**, typ **regedit** en klik dan op **OK**. Ga in het venster **Register-editor** naar `My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`.
4. Stel de waarde **forceguest** in op 0 (de standaardwaarde is 1). Als u deze waarde niet wijzigt, heeft de externe gebruiker die op afstand verbinding maakt met het systeem alleen gastbevoegdheden, zelfs als de opgegeven referenties administratorbevoegdheden geven.
 - a. Maak een account op het clientsysteem met dezelfde gebruikersnaam en hetzelfde wachtwoord, als een Administrator-account op het systeem waarop de beheerapplicatie WMI wordt uitgevoerd.
 - b. Als u gebruik maakt van IT Assistant, voert u het IT Assistant-hulpprogramma ConfigServices (`configservices.exe` in de map/bin in de installatiemap van IT Assistant) uit. Configureer IT Assistant voor uitvoering onder een lokale Administrator-account, die nu ook een administrator op de externe client is. Controleer ook of DCOM en CIM zijn ingeschakeld.
 - c. Als u IT Assistant gebruikt, gebruikt u de administrator-account om de subnetdetectie voor het clientsysteem te configureren. Voer de gebruikersnaam in als <clientcomputernaam>\<accountnaam>. Als het systeem al is gedetecteerd, moet u het systeem uit de lijst met gedetecteerde systemen verwijderen, subnetdetectie voor het systeem configureren en het systeem vervolgens opnieuw detecteren.

OPMERKING: Dell raadt u aan Dell OpenManage Essentials te gebruiken als vervanging voor IT Assistant. Meer informatie over Dell OpenManage Essentials vindt u op dell.com/support.

5. Voer de volgende stappen uit om de bevoegdheidsniveaus voor de gebruiker te wijzigen voor externe verbindingen met de WMI van een systeem:

- a. Klik op **Start > Uitvoeren**, typ `compmgmt.msc` en klik dan op **OK**.
 - b. Ga naar **WMI Control** onder **Services en toepassingen**.
 - c. Klik met de rechtermuisknop op **WMI Control** en klik dan op **Eigenschappen**.
 - d. Klik op het tabblad **Beveiliging** en selecteer **DCIM/SYSMAN** onder de **Root**-structuur.
 - e. Klik op **Beveiliging**.
 - f. Selecteer de specifieke groep of gebruiker die u toegangscontrole wilt geven en gebruik de selectievakjes **Toestaan** of **Weigeren** om de machtigingen te configureren.
6. Voer de volgende stappen uit om verbinding te maken met een WMI (`root\DCIM\SYSMAN`) op een systeem vanaf een extern systeem met WMI CIM Studio:
- a. Installeer WMI-tools samen met `wbemtest` op het lokale systeem en installeer vervolgens Dell Command | Monitor op het externe systeem.
 - b. Configureer de firewall op het systeem voor WMI externe connectiviteit. Open bijvoorbeeld de TCP-poorten 135 en 445 in Windows Firewall.
 - c. Stel de lokale beveiligingsinstelling in op **Klassiek - lokale gebruikers als zichzelf verifiëren voor Netwerktogegang: Model voor delen en beveiliging van lokale accounts** in het **Lokaal beveiligingsbeleid**.
 - d. Maak verbinding met de WMI (`root\DCIM\SYSMAN`) op het lokale systeem vanaf een extern systeem met behulp van WMI `wbemtest`. Bijvoorbeeld: `\\[IP-adres van extern doelsysteem]\root\DCIM\SYSMAN`
 - e. Voer wanneer u hierom wordt gevraagd de administrator-referenties van het externe doelsysteem in.
- Zie de relevante Microsoft-documentatie op msdn.microsoft.com voor meer informatie over WMI.

Installatiefout op systemen waarop Windows wordt uitgevoerd

Als u er niet in slaagt de installatie van Dell Command | Monitor te voltooien, controleer dan het volgende:

- U hebt administratorbevoegdheden op het doelsysteem.
 - Het doelsysteem is een door Dell gemaakt systeem met SMBIOS versie 2.3 of hoger.
 - De PowerShell-console mag niet geopend zijn.
- i** **OPMERKING:** U kunt de SMBIOS-versie van het systeem weergeven door naar **Start > Uitvoeren** te gaan en het bestand `msinfo32.exe` uit te voeren. U vindt de SMBIOS-versie op de pagina **Systeemoverzicht**.
- i** **OPMERKING:** Er moet een ondersteund Windows-besturingssysteem worden uitgevoerd op het systeem.
- i** **OPMERKING:** Het systeem moet voorzien zijn van .NET 4.0 of een hogere versie.

Inventarisatiewaarde van BIOS-instelling wordt weergegeven als 1

1. Controleer of de volgende pakketten zijn geïnstalleerd met de hoofdgebruikersprivileges;
 - `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. Als bovenstaande pakketten zijn geïnstalleerd, controleert u of de drivermodule is geladen.
 - a. Controleer of de drivermodule is geladen door de volgende opdracht uit te voeren `lsmod | grep dcdbas`.
 - b. Als de drivermodule niet beschikbaar is, haalt u de driverinformatie op door de volgende opdracht uit te voeren `modinfo dcdbus`.
 - c. Laad de drivermodule met de volgende opdracht: `insmod <filename>`.

Hapi-installatie mislukt vanwege de afhankelijkheid van libsmbios

Als de installatie mislukt vanwege afhankelijkheidsproblemen, doet u het volgende:

Installeer alle afhankelijke pakketten met de opdracht `apt-get -f install`.

CIM-resource niet beschikbaar

Als u tijdens het inventariseren een foutbericht "CIM-resource niet beschikbaar" ziet:

Controleer of de opdrachten worden uitgevoerd met hoofdmapprivileges.

Kan opdrachten niet uitvoeren met behulp van DCM op de systemen met Ubuntu Core 16

Controleer of de snap-versie op het systeem 2.23 of later is.

Andere documenten die u misschien nodig hebt

Behalve deze gebruikershandleiding kunt u ook de volgende documenten raadplegen op dell.com/support. Klik op Dell Command | Monitor (voorheen OpenManage Client Instrumentation) en klik dan op de juiste productversiekoppeling in de sectie **Algemene support**.

Behalve deze gebruikershandleiding kunt u ook de volgende handleidingen raadplegen.

- De Dell Command | Monitor naslaggids bevat gedetailleerde informatie over alle klassen, eigenschappen en beschrijvingen.
- De Dell Command | Monitor installatiehandleiding bevat informatie over de installatie.
- De Dell Command | Monitor SNMP-naslaggids bevat informatie over SNMP (Simple Network Management Protocol) MIB (Management Information Base) zoals van toepassing op Dell Command | Monitor.

Onderwerpen:

- [Documenten openen op de Dell supportwebsite](#)

Documenten openen op de Dell supportwebsite

U kunt ook de benodigde documenten zoeken door het product te selecteren.

1. Ga naar www.dell.com/manuals.
2. Klik op **Door alle producten bladeren**, klik op **Software** en klik vervolgens op **Clientsysteembeheer**.
3. Als u de vereiste documenten wilt weergeven, klikt u op de gewenste productnaam en het versienummer.

Contact opnemen met Dell

 **OPMERKING:** Als u niet over een actieve internetverbinding beschikt, kunt u contactgegevens vinden op de factuur, de pakbon of in de productcatalogus van Dell.

Dell biedt verschillende online en telefonische ondersteuningsdiensten en -mogelijkheden. De beschikbaarheid verschilt per land en product en sommige services zijn mogelijk niet beschikbaar in uw regio. Om contact op te nemen met Dell voor zaken op het gebied van verkoop, technische ondersteuning of klantenservice:

1. Ga naar **Dell.com/support**.
2. Selecteer uw ondersteuningscategorie.
3. Zoek naar uw land of regio in het vervolgkeuzemenu **Kies een land/regio** onderaan de pagina.
4. Selecteer de gewenste dienst- of ondersteuningslink.