Dell Command | Monitor Version 10.6

Guide de l'utilisateur

Octobre 2021
Rév. A01

Remarques, précautions et avertissements

REMARQUE : Une REMARQUE indique des informations importantes qui peuvent vous aider à mieux utiliser votre produit.

PRÉCAUTION : ATTENTION vous avertit d'un risque de dommage matériel ou de perte de données et vous indique comment éviter le problème.

AVERTISSEMENT : un AVERTISSEMENT signale un risque d'endommagement du matériel, de blessure corporelle, voire de décès.

Table des matières

1

Présentation de Dell Command | Monitor 10.6

L'application logicielle Dell Command | Monitor permet aux administrateurs informatiques de gérer facilement l'inventaire des flottes, de surveiller la santé du système, de modifier les paramètres du BIOS et de collecter à distance des informations pour les systèmes clients Dell déployés.

La surveillance de l'état de santé du système actif peut vous aider à réduire le coût total de possession du système et s'inscrit dans une approche globale de gestion de tous les appareils en réseau.

Dell Command | Monitor est conçu pour les systèmes clients Dell Enterprise, les systèmes Dell IoT Gateway et pour les PC Dell Embedded.

Ce document fournit une présentation de Dell Command | Monitor et de ses diverses fonctionnalités. Pour plus d'informations sur les systèmes Dell pris en charge, consultez les notes de mise à jour disponibles sur **dell.com/support**.

Sujets :

Nouveautés de cette version Dell Command | Monitor 10.6

- Prise en charge des nouveaux attributs du BIOS suivants :
  - `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`
- Prise en charge de la méthode **ResetBIOSDefaults**.

Dell Command | Monitor présentation

REMARQUE : Le protocole SNMP (Simple Network Management Protocol) n'est pas pris en charge par Dell Command | Monitor pour Linux.

Dell Command | Monitor gère les systèmes clients à l'aide des protocoles de gestion suivants : le modèle CIM (Common Information Model) standard et le protocole SNMP (Simple Network Management Protocol). Cela permet de réduire le coût total de possession du système, d'améliorer la sécurité et cela fournit une approche globale pour gérer tous les appareils au sein d'un périphérique réseau.

Grâce au modèle CIM, vous pouvez accéder à Dell Command | Monitor via WSMAN (Web Services for Management Standards).

Dell Command | Monitor contient l'ensemble de pilotes sous-jacents, qui collecte des informations relatives au système client à partir de différentes sources, y compris le BIOS, CMOS, System Management BIOS (SMBIOS), SMI (System Management Interface), le système d'exploitation et les interfaces de programmation d'application (API). Dell Command | Monitor pour Windows collecte également des informations sur le système client à partir de la bibliothèque de liens dynamiques (DLL) et des paramètres de registre. Dell Command | Monitor pour Windows récupère ces informations via l'interface CIMOM (CIM Object Manager), la pile WMI (Windows Management Instrumentation) ou l'agent SNMP. Pour Linux, Dell Command | Monitor récupère ces informations via l'interface OMI (Open Management Infrastructure).

Dell Command | Monitor permet aux administrateurs IT de collecter à distance des informations relatives aux ressources, de modifier les paramètres du BIOS, de recevoir des notifications proactives en cas de risques de pannes et des alertes en cas de failles de sécurité. Sur les systèmes exécutant Windows, ces alertes sont disponibles sous forme d'événements dans le journal des événements NT, d'événements WMI ou d'interruptions SNMP v1. Pour les systèmes exécutant Linux, ces alertes sont reçues sous forme d'événements Syslog, d'événements OMI ou de journal d'application.

Dell Command | Monitor pour Windows peut être intégré à une console telle que MSCCM (Microsoft System Center Configuration Manager), en accédant directement aux informations CIM, ou via d'autres fournisseurs de consoles ayant mis en œuvre l'intégration de Dell Command | Monitor. De plus, vous pouvez créer des scripts personnalisés pour cibler des zones d'intérêt particulières. Des exemples de scripts sont disponibles dans la bibliothèque de connaissances Dell, sur la page Dell Command | Monitor. Vous pouvez utiliser ces scripts pour contrôler l'inventaire, les paramètres du BIOS et l'intégrité du système.

REMARQUE : L'installation par défaut n'active pas la prise en charge SNMP. Pour plus d'informations sur l'activation de la prise en charge de SNMP pour Dell Command | Monitor pour Windows, consultez le Guide d'installation de Dell Command | Monitor sur **dell.com/support**.

2

Section Conformité du document Windows SMM Security Mitigations Table (WSMT)

Le document Windows (SMM) Security Mitigations Table contient des informations sur l table ACPI créée pour le système d'exploitation Windows, qui prend en charge les fonctions de sécurité basée sur la virtualisation (VBS) de Windows. Dell Command | Monitor est compatible avec WSMT. Ce système est utilisé pour la configuration des fonctions de la plate-forme sur les systèmes clients Dell avec BIOS optimisé pour WSMT.

Vous trouverez ci-dessous le changement de comportement lié à la conformité WSMT :

Les fonctionnalités de Dell Command | Monitor sont disponibles sur les plates-formes client Dell qui disposent d'une version du BIOS compatible prenant en charge WMI/ACPI.

REMARQUE : Pour plus d'informations les plates-formes prises en charge, voir Plates-formes prises en charge.

3

Normes et protocoles pour Dell Command | Monitor 10.6

Dell Command | Monitor est basé sur les normes CIM. La spécification CIM détaille des techniques d'adressage permettant une compatibilité améliorée avec des protocoles de gestion.

Des protocoles de gestion tels que WMI, SNMP et WSMAN sont utilisés pour la surveillance à distance.

REMARQUE : Dell Command | Monitor pour Windows utilise le protocole SNMP (Simple Network Management Protocol) pour décrire plusieurs variables du système.

Le DMTF (Distributed Management Task Force) est le corps de normes reconnu dans l'industrie qui dirige le développement, l'adoption et l'unification des normes de gestion (notamment CIM et ASF) et les initiatives pour les environnements de bureau, d'entreprise et Internet.

4

Scénarios de cas d'utilisation à l'aide de Dell Command | Monitor 10.6

Cette section décrit les divers scénarios d'utilisation de Dell Command | Monitor.

Vous pouvez utiliser Dell Command | Monitor pour :

- Gestion de parc informatique
- Gestion de la configuration
- Surveillance de l'intégrité
- Profils

Sujets :

Scénario 1 : Gestion de parc informatique

Une société disposant de nombreux systèmes Dell n'a pas pu conserver des informations d'inventaire précises, car le personnel informatique et de l'entreprise a changé. Le responsable informatique (CIO) demande un plan d'identification des systèmes pouvant être mis à niveau vers la dernière version de Windows. Cela nécessite une évaluation des systèmes déployés afin de déterminer la taille, le périmètre et l'impact financier d'un tel projet. La collecte d'informations engendre des efforts considérables. Le déploiement de personnel informatique sur chaque système client est coûteux en termes d'interruptions chez l'utilisateur final.

Grâce à l'utilisation de Dell Command | Monitor sur chaque système Dell, le responsable IT peut rapidement collecter des informations à distance. Grâce à l'utilisation d'outils tels que Microsoft System Center Configuration Manager (SCCM), le responsable informatique interroge chaque système client sur le réseau et collecte des informations telles que le type et la vitesse du processeur, la taille de la mémoire, la capacité du disque dur, la version du BIOS et la version du système d'exploitation actuel. Une fois les informations collectées, elles peuvent être analysées pour identifier les systèmes pouvant être mis à niveau vers la dernière version de Windows.

Vous pouvez également obtenir l'inventaire des ressources via la ligne de commande WSMAN/WinRM ou toute autre ligne de commande du client CIM.

Intégration SCCM

Vous pouvez intégrer SCCM à Dell Command | Monitor pour Windows en :

- Utilisant le fichier MOF du package d'installation de Dell Command | Monitor, qui contient toutes les classes Dell Command | Monitor et en l'important vers ConfigMgr

  Le fichier MOF se trouve à l'emplacement suivant :

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

- étendez les fonctionnalités de rapport d'inventaire à l'aide de collections

Scénario 2 : Gestion de la configuration

Une société prévoit de standardiser la plateforme client et de gérer chaque système tout au long de son cycle de vie. Dans le cadre de cette démarche, la société acquiert une suite d'outils et prévoit d'automatiser le déploiement d'un nouveau système d'exploitation client en utilisant l'environnement de préamorçage (PXE).

Le défi consiste à trouver un moyen de modifier le mot de passe du BIOS de chaque ordinateur client à distance. Lorsque Dell Command | Monitor est installé sur chaque système client, le département IT de la société dispose de différentes options pour modifier la séquence d'amorçage à distance. La console de gestion OpenManage Essentials (OME) peut être intégrée à Dell Command | Monitor et utilisée pour surveiller les paramètres du BIOS à distance sur tous les systèmes clients. Une autre option consiste à écrire un script (CIM, WinRM/WSMAN/PowerShell/WMIC) qui modifie la configuration du BIOS. Le script peut être distribué via le réseau et exécuté sur chaque système client.

Pour plus d'informations sur Dell Command | Monitor, consultez le Guide de référence de Dell Command | Monitor sur **dell.com/support**.

Les configurations standardisées peuvent permettre de réduire considérablement les coûts, quelle que soit la taille de l'entreprise. De nombreuses entreprises déploient des systèmes clients standardisés, mais peu d'entre elles gèrent la configuration système tout au long du cycle de vie de l'ordinateur. Avec Dell Command | Monitor installé sur chaque système client, le département IT peut verrouiller les ports hérités afin de prévenir l'utilisation de périphériques non autorisés ou activer WOL (Wake On LAN) pour sortir le système d'un état de veille afin d'effectuer des tâches de gestion d'administration.

Scénario 3 : Surveillance de l'intégrité

Un utilisateur reçoit des messages d'erreur de lecture alors qu'il tente d'accéder à certains fichiers sur le disque dur du système client. L'utilisateur redémarre le système et les fichiers semblent désormais accessibles. L'utilisateur ignore le problème initial, car il semble se résoudre de lui-même. Pendant ce temps, Dell Command | Monitor interroge le disque dur sur le problème pour une défaillance prévue et transmet une alerte SMART (Self-Monitoring, Analysis and Reporting Technology) à la console de gestion. Elle affiche également l'erreur SMART à l'utilisateur local. L'alerte indiquait que plusieurs erreurs de lecture/écriture se produisent sur le disque dur. Le département IT de la société a recommandé que l'utilisateur effectue immédiatement une sauvegarde des fichiers de données stratégiques. Un technicien de service est envoyé avec un disque de remplacement.

Le disque dur est remplacé avant de tomber en panne, ce qui prévient tout interruption de service, un appel au centre d'assistance et le déplacement d'un technicien en vue de diagnostiquer le problème.

TranslatedSurveillance des alertes système via l'Observateur d'événements du système d'exploitation, Syslog ou l'indication CIM

Dell Command | Monitor prend en charge la surveillance des événements à l'aide des procédures suivantes :

- Extraction du journal par l'intermédiaire de la classe CIM DCIM_LogEntry.
- Surveillance de l'indication CIM par l'intermédiaire de la classe DCIM_AlertIndication.
- (Uniquement pour Dell Command | Monitor pour Windows) Surveillance des événements via le protocole SNMP (Simple Network Management Protocol [protocole de gestion de réseau simple]) et l'observateur d'événements Windows.
- (Uniquement pour Dell Command | Monitor pour Linux) Surveillance via Syslog.

Pour plus d'informations sur Dell Command | Monitor, consultez le Guide de référence de Dell Command | Monitor sur **dell.com/support**.

Scénario 4 : Profils

REMARQUE : Les profils DMTF sont mis en oeuvre pour Dell Command | Monitor uniquement pour Windows.

Les administrateurs informatiques doivent gérer les systèmes clients dans des environnements d'entreprise multifournisseurs et distribués. Ils doivent maîtriser un ensemble d'outils et d'applications tout en gérant plusieurs systèmes clients de postes de travail ou ordinateurs portables dans divers réseaux. Afin de réduire le coût engendré par ces exigences et représenter les données de gestion fournies, les profils DMTF (Distributed Management Task Force) et DCIM-OEM (Data Center Infrastructure Management) sont mis en œuvre dans Dell Command | Monitor. Certains profils DMTF sont expliqués dans ce guide.

Pour plus d'informations sur Dell Command | Monitor, consultez le Guide de référence de Dell Command | Monitor sur **dell.com/support**.

Profil des actifs

État de la garantie sur l'appareil du point de terminaison :

- Déterminez l'état de la garantie en énumérant/obtenant l'instance de la classe **DCIM_AssetWarrantyInformation**.
- Vérifiez que l'état de la garantie peut être déterminé à l'aide des propriétés **WarrantyStartDate** et **WarrantyEndDate** de la classe **DCIM_AssetWarrantyInformation**.

REMARQUE : Vous devez disposer d'une connexion Internet opérationnelle pour utiliser DCIM_AssetWarrantyInformation. Si vous exécutez Dell Command | Monitor derrière un serveur proxy, assurez-vous que les paramètres de proxy sont correctement configurés.

Pour obtenir plus d'informations sur l'état de garantie des périphériques :

1. Rendez-vous sur Dell.com/support.
2. Recherchez votre pays ou zone géographique dans la liste déroulante « Choisissez un pays ou une zone géographique » située au bas de la page.
3. Sélectionnez la catégorie de support Garantie et contrats.
4. Affiche le numéro de série approprié de l'ordinateur.

- Désactivez la fonctionnalité de garantie et les demandes d'actualisation ultérieures.
- Extrayez les informations de garantie à la demande.

REMARQUE : Les informations sur la garantie sont mises à jour automatiquement tous les 15 jours. Dans le cas d'un état de garantie récent, les informations de garantie énumérées peuvent ne pas être identiques à celles indiquées sur le site de support Dell.

Profil de batterie

- Déterminez l'état de la batterie en énumérant/obtenant l'instance de la classe **DCIM_Battery**.
- Déterminez le temps d'exécution estimé et notez la charge estimée restante.
- Vérifiez si les informations d'intégrité de la batterie peuvent être déterminées à l'aide des propriétés État opérationnel et État d'intégrité de la classe **DCIM_Battery**.
- Obtenez des informations supplémentaires sur l'intégrité d'une batterie à l'aide de la propriété **DCIM_Sensor.CurrentState** ou de la propriété **CIM_NumericSensor.CurrentState**.
- Déterminez l'emplacement de la batterie et l'ePPID de la batterie à l'aide des propriétés **Identification des descriptions** et **Autres informations d'identification** de la classe **DCIM_Battery**.

DCIM_Battery

Pour obtenir des informations sur la valeur ePPID de la batterie pour un élément de batterie : ouvrez une invite PowerShell avec les privilèges d'administration, puis exécutez la commande suivante `Get-CimInstance -Namespace root/dcim/sysman -Classname DCIM_Battery |Select ElementName, OtherIdentifyingInfo, IdentifyingDescriptions.`

REMARQUE : La valeur ePPID de la batterie n'est pas dynamique. Si la batterie est remplacée, vous devez redémarrer le système pour qu'il tienne compte des modifications apportées à l'instance **DCIM_Battery**.

Profil de gestion du BIOS

- Déterminez la version du BIOS en énumérant l'instance de la classe **DCIM_BIOSElement**.
- Assurez-vous que les valeurs d'attribut du BIOS peuvent être modifiées ou non. Obtenez l'instance de la classe **DCIM_BIOSEnumeration**. L'attribut peut être modifié si la propriété **IsReadOnly** est définie sur FALSE.
- Définissez le mot de passe du système (SystemPwd). Exécutez la méthode **DCIM_BIOSService.SetBIOSAttributes()** et définissez le SystemPwd sur AttributeName et la valeur du mot de passe sur les paramètres AttributeValue.
- Définissez le mot de passe du BIOS ou de l'administrateur (AdminPwd). Exécutez la méthode **DCIM_BIOSService.SetBIOSAttributes()** et définissez l'AdminPwd sur AttributeName et la valeur du mot de passe sur les paramètres AttributeValue.
- Exécutez la méthode **DCIM_BIOSService.SetBIOSAttribute()**, puis spécifiez les paramètres AttributeName et AttributeValue.
- Pour modifier un attribut BIOS lors de la définition du mot de passe BIOS/Admin, exécutez la méthode **DCIM_BIOSService.SetBIOSAttribute()**, puis spécifiez le nom d'attribut et la valeur d'attribut (AtributeName et AttributeValue) et le mot de passe BIOS actuel comme paramètre d'entrée de jeton d'autorisation (AuthorizationToken).

Contrôle du démarrage

- Modifiez la séquence des éléments de démarrage dans la liste de démarrage héritée et UEFI.
- Activez ou désactivez les éléments de démarrage dans la liste de démarrage héritée et UEFI.
- Cherchez la configuration d'amorçage actuelle en énumérant les instances de la classe **DCIM_ElementSettingData** dont la propriété **IsCurrent** est définie sur **1**. L'instance **DCIM_BootConfigSetting** représente la configuration d'amorçage actuelle.

Mobile d'ordinateur de bureau de base

- Déterminez le modèle du système, le numéro de service et le numéro de série en énumérant l'instance de la classe **DCIM_ComputerSystem**.
- Vous pouvez utiliser la méthode **DCIM_ComputerSystem.RequestStateChange()** pour définir la valeur du paramètre RequestedState sur **3**. La valeur de paramètre 3 éteint le système.
- Vous pouvez utiliser la méthode **DCIM_ComputerSystem.RequestStateChange()** pour définir la valeur du paramètre **RequestedState** sur **11**. La valeur de paramètre 11 redémarre le système.
- Déterminez l'état d'alimentation du système.
- Déterminez le nombre de processeurs du système en interrogeant **DCIM_Processor**, instances qui sont associées à l'Instance centrale par l'intermédiaire de l'association **DCIM_SystemDevice**.
- Obtenez l'heure du système. Exécutez la méthode **DCIM_TimeService.ManageTime()** et définissez le paramètre **GetRequest** sur **True**.
- Vérifiez l'état d'intégrité de l'élément géré.

Enregistrement du journal

- Identifiez le nom du journal en sélectionnant l'instance **DCIM_RecordLog** dont la propriété **ElementName** correspond au nom du journal.
- Cherchez les entrées de journal individuelles. Obtenez toutes les instances de **DCIM_LogEntry** associées à l'instance donnée de **DCIM_RecordLog** via l'association **DCIM_LogManagesRecord** . Triez les instances en fonction de **RecordID**.
- Vérifiez si les journaux d'enregistrement sont activés en énumérant l'instance de la classe **DCIM_RecordLog** dont la propriété **Enabledstate** est définie sur **2** (Activée) et la propriété **EnabledState** est définie sur **3** (Désactivée).
- Triez les enregistrements de journal en fonction de l'horodatage de l'entrée de journal. Obtenez toutes les instances de **DCIM_LogEntry** associées à l'instance donnée de **DCIM_RecordLog** via l'association **DCIM_LogManagesRecord** . Triez les instances de **DCIM_LogEntry** en fonction de la valeur de propriété **CreationTimeStamp** dans l'ordre du dernier arrivé, premier sorti (LIFO).
- Nettoyez les journaux en exécutant la méthode **ClearLog()** correspondant à l'instance donnée de **DCIM_RecordLog**.

Inventaire physique

- Obtenez l'inventaire physique de tous les périphériques au sein d'un système.
- Obtenez l'inventaire physique d'un châssis du système.
- Déterminez le numéro de référence d'un composant défaillant.
- Déterminez si le logement est vide ou non.

Profil de mémoire système

- Recherchez les informations de mémoire du système.
- Recherchez les informations de mémoire physique du système.
- Vérifiez la taille de la mémoire système.
- Vérifiez la taille de la mémoire système disponible.
- Vérifiez la taille de la mémoire système physique disponible.
- Vérifiez l'état d'intégrité de la mémoire système.

5

Avec Dell Command | Monitor 10.6

Vous pouvez afficher les informations fournies par Dell Command | Monitor en vous rendant sur : `root\dcim\sysman (standard)`

Dell Command | Monitor fournit les informations par l'intermédiaire de classes dans ces espaces de nom.

Pour plus d'informations sur les classes, consultez le Guide de référence de Dell Command | Monitor sur **dell.com/support**.

Sujets :

Configuration de l'intervalle d'interrogation

Vous pouvez modifier l'intervalle d'interrogation de la sonde du ventilateur, la sonde de température, la sonde de tension, la sonde actuelle, l'augmentation/réduction de la volumétrie, l'augmentation/réduction de la mémoire et l'augmentation/réduction du nombre de processeurs à l'aide de Dell Command | Monitor.

- Pour Windows, le fichier `dcsbdy32.ini` ou `dcsbdy64.ini` se trouve sous `<Dell Command | Monitor installed location>\omsa\ini`.
- Pour Linux, le fichier `AlertPollingSettings.ini` se trouve se trouve sous `/opt/dell/dcm/conf`.

REMARQUE : Les nombres contenus dans le fichier INI sont des multiples de **23**. L'intervalle d'interrogation par défaut pour la volumétrie, l'alerte SMART (Self-Monitoring, Analysis and Reporting Technology) est de **626** secondes (temps réel = 626 X 23 secondes, ce qui équivaut approximativement à 3 heures).

Rapport d'état RAID

Dell Command | Monitor permet d'activer les informations de configuration RAID et surveille les fonctionnalités RAID des systèmes clients bénéficiant du support matériel et pilote. Vous pouvez utiliser des classes RAID pour recevoir les détails des niveaux de RAID, des informations sur les pilotes, de la configuration du contrôleur et de l'état du contrôleur. Une fois la configuration RAID activée, vous pouvez recevoir des alertes en cas de dégradation ou de défaillance des disques et des contrôleurs.

REMARQUE : La création de rapport sur l'état RAID est prise en charge uniquement pour les contrôleurs RAID qui fonctionnent sur les pilotes conformes à Common Storage Management Interface (CSMI) version 0.81. OMCI 8.1 et ses versions ultérieures prennent en charge la surveillance du contrôleur RAID sur puce Intel uniquement ; et OMCI 8.2 et ses versions ultérieures prennent en charge les alertes du contrôleur RAID sur puce Intel.

Surveillance des systèmes clients Dell

- Dell Command | Monitor pour Windows prend en charge le protocole SNMP (Simple Network Management Protocol) pour la surveillance et la gestion de systèmes clients tels que des ordinateurs portables, des ordinateurs de bureau et des stations de travail. Le fichier MIB (Management Information Base) est partagé entre Dell Command | Monitor et Server Administrator. Dell Command | MonitorÀ partir de la version 9.0, Dell Command | Monitor pour Windows a été modifié pour utiliser un OID spécifique au client OID (10909) pour que les consoles identifient les systèmes clients.

Pour en savoir plus sur SNMP, consultez le Guide de référence SNMP de Dell Command | Monitor sur **dell.com/support**.

- Dell Command | Monitor pour Linux prend en charge la surveillance à l'aide des commandes WinRM et WSMan.

Journal d'application de Dell Command | Monitor pour Linux

Dell Command | Monitor pour Linux sépare les journaux d'application et les alertes pour permettre la création de rapports et le débogage. L'historique des alertes et des journaux créés pour l'application Dell Command | Monitor est consultable dans le fichier **dcm_application.log** accessible sous `/opt/dell/dcm/var/log`.

Fichier de configuration

Vous pouvez mettre à jour le fichier de configuration **log.property** accessible sous `/opt/dell/dcm/conf` pour appliquer les paramètres souhaités et choisir DEBUG :

REMARQUE : Après avoir modifié le fichier de configuration, redémarrez le serveur OMI pour appliquer les modifications.

- Log_Level : trois niveaux de journalisation ont été définis pour séparer les messages du système : ERROR, INFO, DEBUG.

  L'utilisateur peut changer le niveau de journalisation en modifiant le fichier de configuration. Si le niveau de journalisation défini est DEBUG, le journal de l'application Dell Command | Monitor enverra toutes les informations au fichier journal indiqué.

  REMARQUE : Le niveau de journalisation par défaut est INFO.
- File_Size : l'utilisateur peut définir la taille maximale du fichier **dcm_application.log**. La taille par défaut du fichier est 500 Mo.

  REMARQUE : La valeur File_Size doit être exprimée en octets.
- BackupIndex : l'utilisateur peut définir le nombre de rotations du fichier **dcm_application.log**. Si le nombre de rotations par défaut est 2, le troisième fichier de sauvegarde remplace le fichier le plus ancien.

Détection des disques à format avancé

Les systèmes clients sont en train de passer à des disques de format avancé (AF) pour bénéficier d'une capacité de stockage supérieure et pour répondre aux limitations des disques durs secteur (HDD) de 512 octets. Le passage à des disques durs secteur de 4 Ko permet de garder la compatibilité descendante, tandis que le disque dur AF actuel, connu sous le nom de disque dur 512e, correspondent à 512 octets SATA et fonctionnent à 4 Ko. Lors de la transition, vous pouvez rencontrer des problèmes de performance tels que la partition des disques mal alignés dans les systèmes clients, entraînant la défaillance des packages logiciels de chiffrement basés sur secteur qui gèrent les disques 512e. Dell Command | Monitor vous permet de déterminer si le disque dur d'un système est un disque AF 4 Ko, ce qui aide à éviter les problèmes énumérés précédemment.

Configurations de démarrage

REMARQUE : Dell Command | Monitor pour Linux n'offre pas les capacités de configuration de démarrage. Cette section ne s'applique donc pas à Dell Command | Monitor pour Linux.

Un système client peut avoir l'un de ces deux types de configuration de démarrage :

- Hérité (BIOS)
- UEFI

Dans Dell Command | Monitor, la configuration de démarrage (existante ou UEFI) est modélisée à l'aide des classes suivantes :

- DCIM_ElementSettingData
- DCIM_BootConfigSetting
- DCIM_OrderedComponent
- DCIM_BootSourceSetting
- DCIM_SmartAttributeInfo

REMARQUE : Ici, les expressions Configuration d'amorçage et Type de liste d'amorçage sont utilisées de façon interchangeable et ont la même signification qu'il s'agisse de la configuration Héritée ou UEFI.

DCIM_AssetWarrantyInformation

- Pour interroger l'état de la garantie sur l'appareil du point de terminaison, exécutez la commande suivante dans l'invite PowerShell :

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

- Pour répertorier les droits de garantie par ordre chronologique `WarrantyEndDate`, exécutez la commande suivante dans l'invite PowerShell :

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

- Pour désactiver la fonctionnalité de garantie et les demandes d'actualisation ultérieures, exécutez la commande suivante dans l'invite PowerShell :

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

- Pour extraire des informations sur la garantie à la demande, exécutez la commande suivante dans l'invite PowerShell :

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

REMARQUE : installation pour la configuration du proxy —

- Proxy par défaut : Dell Command | Monitor sélectionne le proxy système par défaut (défini dans IE)
- Proxy personnalisé

  La classe **DCIM_ApplicationProxySetting** est utilisée pour modifier les paramètres de proxy de Dell Command | Monitor en fonction de l'environnement proxy.

DCIM_BootConfigSetting

Une instance de **DCIM_BootConfigSetting** représente une configuration d'amorçage utilisée au cours du processus de démarrage. Par exemple, sur les systèmes clients, il existe deux types de configuration d'amorçage : existante et UEFI. Par conséquent, **DCIM_BootConfigSetting** a un maximum de deux instances à représenter, une pour le type existant et une pour le type UEFI.

Vous pouvez déterminer si **DCIM_BootConfigSetting** représente Hérité, à l'aide des propriétés suivantes :

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

Vous pouvez déterminer si **DCIM_BootConfigSetting** représente UEFI, à l'aide des propriétés suivantes :

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

DCIM_BootSourceSetting

Cette classe représente les périphériques d'amorçage ou les sources. Les propriétés **ElementName**, **BIOSBootString** et **StructuredBootString** contiennent une chaîne qui identifie les périphériques d'amorçage. Par exemple : disquette, disque dur, CD/DVD, réseau, Personal Computer Memory Card International Association (PCMCIA), véhicule électrique à batterie (VEB) ou périphérique USB. Selon le type de liste de démarrage du périphérique, une instance de **DCIM_BootSourceSetting** est associée à l'une des instances de **DCIM_BootConfigSetting**.

DCIM_OrderedComponent

La classe d'association **DCIM_OrderedComponent** est utilisée pour associer les instances de **DCIM_BootConfigSetting** à des instances de **DCIM_BootSourceSetting** représentant l'un des types de liste de démarrage (existante ou UEFI) auquel les périphériques de démarrage appartiennent. La propriété **GroupComponent** de **DCIM_OrderedComponent** fait référence à l'instance **DCIM_BootConfigSetting** et la propriété **PartComponent** fait référence à l'instance **DCIM_BootSourceSetting**.

DCIM_Attribut Smart

Pour lire la valeur de l'attribut SMART, exécutez les commandes suivantes :

Par exemple :

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

Pour configurer les valeurs seuils personnalisées, exécutez les commandes suivantes :

Par exemple :

- Get-CimInstance -Namespace root\dcim\sysman DCIM_SmartAttributeInfo -Filter "AttributeID like '<Attribute ID Value>'" | Invoke-CimMethod -MethodName "SetCustomThreshold" -Arguments @{CustomThresholdValue="<seuil personnalisé à définir>"}

DCIM_ThermalInformation

DCIM_ThermalInformation gère les paramètres de configuration thermique tels que le Mode thermique, le Mode AAC et le Mode de défaillance du ventilateur.

- Pour interroger les données thermiques de l'appareil, exécutez la commande suivante :

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

- Pour définir la valeur du Mode thermique, exécutez la commande suivante :

```
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")}
```

Modification des paramètres système

Dans Dell Command | Monitor, utilisez les méthodes suivantes pour modifier les paramètres système et l'état des systèmes locaux ou distants :

- SetBIOSAttributes : modifie le paramètre BIOS

  REMARQUE : Dell Command | Monitor pour Linux ne prend actuellement en charge que la méthode SetBIOSAttributes.
- ChangeBootOrder : modifie la configuration d'amorçage
- RequestStateChange : arrête et redémarre le système
- ManageTime : affiche l'heure du système

Dans Dell Command | Monitor pour Windows, vous pouvez exécuter ces méthodes en utilisant winrm, un script VB, des commandes PowerShell, wmic et WMI wbemtest.

Réinitialisation des paramètres par défaut du BIOS pour les systèmes s'exécutant sous Windows ou Linux

ResetBIOSDefaults (méthode)

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

Commande 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> }`

Les valeurs possibles sont :

- 0- Paramètres de sécurité par défaut intégrés : il s'agit des paramètres par défaut du BIOS. Cette configuration prend en charge toutes les plates-formes. Par conséquent, la configuration ne peut pas être modifiée.

- 1- Dernière valeur correcte connue : cette opération est générée automatiquement par le BIOS lorsque le POST a réussi. Cette option rétablit la configuration du BIOS. Si les **Paramètres de sécurité par défaut intégrés** sont corrompus, vous pouvez utiliser l'option **Dernière valeur correcte connue** pour restaurer le BIOS.
- 2- Paramètres par défaut : les paramètres par défaut sont générés avant l'expédition du système. Cette configuration est optimisée pour la configuration matérielle ou personnalisée en fonction de vos besoins lors de l'achat ou du service.
- 3- Configuration utilisateur 1 : cette option est configurée lorsque l'utilisateur le demande. Vous devez **Enregistrer la configuration actuelle** dans la configuration du BIOS ou sur l'écran F2 pour réinitialiser la configuration via l'application Dell Command | Monitor.
- 4- Configuration utilisateur 2 : cette option est configurée lorsque l'utilisateur le demande. Vous devez **Enregistrer la configuration actuelle** dans la configuration du BIOS ou sur l'écran F2 pour réinitialiser la configuration via l'application Dell Command | Monitor.

Tableau 1. Valeurs possibles lors de la réinitialisation des paramètres par défaut du BIOS

Description	Code d'erreur (valeur SetResult)
Succès	0
Valeur d'entrée non valide/Valeur d'entrée hors plage	1
Erreur d'authentification	2
Configuration non prise en charge	3
Configuration vide	4
Échec générique/Échec/lorsque le service n'est pas en cours d'exécution	4294967295

REMARQUE : Un redémarrage du système est nécessaire après l'opération **ResetBIOSDefaults** pour que les modifications soient prises en compte.

Les fenêtres DCM permettent d'arrêter ou de redémarrer le système via les API suivantes :

- Redémarrer le système - `Get-CimInstance -Namespace ROOT\DCIM\SYSMAN -ClassName DCIM_ComputerSystem |Where-Object {$_.Dedicated -ne 28} | Invoke-CimMethod -MethodName RequestStateChange -Arguments @{RequestedState ='11'}`
- Arrêter le système - `Get-CimInstance -Namespace ROOT\DCIM\SYSMAN -ClassName DCIM_ComputerSystem |Where-Object {$_.Dedicated -ne 28} | Invoke-CimMethod -MethodName RequestStateChange -Arguments @{RequestedState ='3'}`

Les API suivantes peuvent être utilisées dans le système d'exploitation GNU ou Linux :

- arrêt -r +5
- redémarrage sudo

REMARQUE : Lors de l'opération de réinitialisation, un sous-ensemble d'options n'est pas réinitialisé sur les paramètres par défaut. Cela peut être pour des raisons de sécurité (des mots de passe, par ex.) ou pour démarrer (liste de démarrage et ROM en option héritée).

Les journaux d'événements du BIOS ne sont pas réinitialisés pour stocker l'historique du matériel du système.

Le tableau suivant énumère la liste complète des fonctionnalités qui ne sont pas réinitialisées aux paramètres par défaut.

Tableau 2. Liste complète des fonctionnalités qui ne sont pas réinitialisées aux paramètres par défaut

Section	Sous-section	Élément
Général	Informations détaillées de	Numéro de série
	Informations détaillées de	Numéro de Numéro d'inventaire
	Informations détaillées de	Étiquette de propriété
	Séquence d'amorçage	Liste d'amorçage
	Options de démarrage avancées	Activer les ROM en option héritée
	Date/Heure	Date/Heure
	Carte NIC intégrée	Carte NIC intégrée
	Carte NIC intégrée	Activer la pile réseau UEFI

Tableau 2. Liste complète des fonctionnalités qui ne sont pas réinitialisées aux paramètres par défaut (suite)

Section	Sous-section	Élément
	SATA Operation (Fonctionnement SATA)	SATA Operation (Fonctionnement SATA)
Sécurité	N/A	Mot de passe administrateur
	N/A	Mot de passe système
	N/A	Mots de passe HDD-x internes
	N/A	Verrouillage du mot de passe maître
	Réduction des risques de sécurité SMM	Réduction des risques de sécurité SMM
	Activer Intel SGX	Activer Intel SGX
Démarrage sécurisé	Activation de Secure Boot	Activation de Secure Boot
	Gestion des clés experte	Bases de données clés

Configuration des attributs du BIOS sur un système exécutant Windows à l'aide de commandes PowerShell

Vous pouvez définir les attributs du BIOS à l'aide de la méthode SetBIOSAttributes. La procédure est expliquée ci-dessous à l'aide d'une tâche d'activation du module TPM (Trusted Platform Module) comme exemple.

REMARQUE : Assurez-vous que l'option module de plateforme sécurisée (TPM) est désactivée dans le BIOS avant de suivre la procédure d'activation du module de plateforme sécurisée (TMP) .

REMARQUE : Utilisez PowerShell avec les privilèges d'administrateur.

Pour activer TPM,

1. Définissez le mot de passe du BIOS sur le système s'il n'est pas défini à l'aide de la commande PowerShell suivante :

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

2. Activez la sécurité TPM à l'aide de la commande suivante :

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

3. Redémarrez le système.
4. Activez le TPM à l'aide de la commande suivante :

   ```
   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. Redémarrez le système.

   Clauses de non-responsabilité générales

   Le module PSReadline du Powershell enregistre chaque commande de la console que vous saisissez dans un fichier texte. Il est donc recommandé d'utiliser la comandlet « Get-Credential » pour gérer les mots de passe en toute sécurité.

   a. $cred = Get-Credential

   b. Saisissez votre nom d'utilisateur et le mot de passe, par exemple, AdminPWD et Dell_123$, lorsque la boîte de dialogue s'affiche.

   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 ")}

Configuration des attributs du BIOS sur un système exécutant Linux

Vous pouvez définir les attributs du BIOS à l'aide des méthodes suivantes :

- Utilisation de OMICLI
- Utilisation de WinRM
- Utilisation de WSMan

REMARQUE : Assurez-vous que le serveur OMI est démarré et en cours d'exécution.

Configuration des attributs du BIOS à l'aide de OMICLI

Vous pouvez définir les attributs du BIOS à l'aide de la méthode SetBIOSAttributes. La procédure est expliquée ci-dessous à l'aide d'une tâche d'activation du module TPM (Trusted Platform Module) comme exemple.

REMARQUE : Assurez-vous que l'option module de plateforme sécurisée (TPM) est désactivée dans le BIOS avant de suivre la procédure d'activation du module de plateforme sécurisée (TMP) .

Pour configurer les attributs du BIOS à l'aide de commandes OMICLI :

1. Pour définir le mot de passe du BIOS sur le système s'il n'est pas déjà défini, exécutez

```
./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. Pour activer la sécurité TPM à l'aide de la commande suivante, exécutez

```
./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. Redémarrez le système.
4. Pour activer le module TPM, exécutez

```
./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. Redémarrez le système.
6. Pour réinitialiser le mot de passe du BIOS, exécutez

```
./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>"  }
```

Configuration des attributs du BIOS à l'aide de WinRM

Vous pouvez définir les attributs du BIOS à l'aide de la méthode SetBIOSAttributes. La procédure est expliquée ci-dessous à l'aide d'une tâche d'activation du module TPM (Trusted Platform Module) comme exemple.

REMARQUE : Assurez-vous que l'option Module de plateforme sécurisée (TPM) est désactivée dans le BIOS avant de suivre la procédure d'activation du module de plateforme sécurisée (TMP).

Pour configurer les attributs du BIOS à l'aide de commandes WinRM :

1. Obtenez le sélecteur défini en énumérant la classe DCIM_BIOSService. Exécuter :

```
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
```

REMARQUE : Les valeurs de définition du sélecteur (SystemName=<system name from DCIM_BIOSService class>winrm i SetBIOSAttributes wsman/DCIM_BIOSService?SystemName=dt :+SystemCreationClassName=DCIM_ComputerSystem+Name=DCIM:BiosService+CreationClassName=DCIM_BIOSService+) sont utilisés pour l'opération de définition dans cet exemple.

2. Définissez le mot de passe du BIOS sur le système s'il n'est pas défini à l'aide de la commande suivante :

```
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. Activez la sécurité TPM en exécutant la commande suivante :

```
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. Redémarrez le système.
5. Activez le TPM à l'aide de la commande suivante :

```
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>"}
```

Configuration des attributs du BIOS à l'aide de WSMan

Vous pouvez définir les attributs du BIOS sur les systèmes exécutant Linux à l'aide de WSMan. La procédure est expliquée ci-dessous à l'aide d'une tâche d'activation du module TPM (Trusted Platform Module) comme exemple.

REMARQUE : Assurez-vous que l'option Module de plateforme sécurisée (TPM) est désactivée dans le BIOS avant de suivre la procédure d'activation du module de plateforme sécurisée (TMP).

1. Obtenez le sélecteur défini en énumérant la classe DCIM_BIOSService. Exécuter :

```
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. Définissez le mot de passe du BIOS sur le système s'il n'est pas défini à l'aide de la commande suivante :

```
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. Activez la sécurité TPM à l'aide de la commande suivante :

```
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. Redémarrez le système.
5. Activez le TPM à l'aide de la commande suivante :

```
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>”
```

Modification de la séquence de démarrage

Pour modifier la séquence de démarrage, suivez les étapes suivantes :

1. Vérifiez le type de séquence d'amorçage (hérité ou UEFI) en utilisant la commande suivante :
   - Commande WMIC : `wmic /namespace:\\root\dcim\sysman path dcim_BootConfigSetting get ElementName/format:list`.
   - Commande PowerShell : `Get-WmiObject -namespace root\dcim\sysman -class dcim_BootConfigSetting -Property ElementName`.
2. Vérifiez le type de séquence d'amorçage actuelle (hérité ou UEFI) en utilisant la commande suivante :
   - Commande WMIC : `wmic /namespace:\\root\dcim\sysman path dcim_ElementSettingData.IsCurrent=1 get SettingData /format:list .`
   - Commande PowerShell : `Get-WmiObject -namespace root\dcim\sysman -class dcim_elementSettingData -Filter "IsCurrent=1" -Property SettingData`.
3. Modification de la séquence d'amorçage en utilisant la commande suivante :
   - Commande WMIC : `wmic /namespace:\\root\dcim\sysman path dcim_bootconfigsetting call ChangeBootOrder /?:full .`
   - Commande PowerShell : `(Get-WmiObject -namespace root\dcim\sysman -class dcim_bootconfigsetting).getmethodparameters("ChangeBootOrder") .`

     REMARQUE : L'instance `dcim_BootConfigSetting` doit représenter la configuration d'amorçage que vous souhaitez modifier : type 1 (existante) ou type 2 (UEFI).
   - Les arguments sont les suivants :
     - `Authorization Token` : il s'agit du mot de passe d'administrateur ou d'amorçage.
     - `Source` : il s'agit de la liste de séquence d'amorçage d'une propriété `dcim_OrderedComponent.PartComponent`. La nouvelle séquence d'amorçage est déterminée par l'ordre des périphériques d'amorçage dans la baie source.
4. Modification de la séquence d'amorçage de la liste d'amorçage type 1 en utilisant PowerShell :
   a. Obtenez la séquence d'amorçage actuelle de la liste d'amorçage type 1 en exécutant la commande suivante : `$boLegacy = Get-WmiObject -namespace root\dcim\sysman -class dcim_orderedcomponent | where {$_.partcomponent -match 'BootListType-1'} | select -expand partcomponent.`
   b. Définissez une variable PowerShell pour spécifier la séquence d'amorçage pour définir `$newboLegacy.` Attribuez-lui la nouvelle séquence d'amorçage. Par exemple, la séquence d'amorçage actuelle est conservée.
   c. $newboLegacy = $boLegacy
   d. Obtenez l'instance `dcim_bootconfigsetting` correspondant à la liste d'amorçage type 1 en exécutant la commande suivante : `$bcsLegacy = Get-WmiObject -Namespace root\dcim\sysman -ClassName dcim_bootconfigsetting | where {$_.ElementName -eq 'Next Boot Configuration Setting : Boot List Type 1'}.`
   e. Lancez la méthode en exécutant la commande suivante : `$ bcsLegacy.changebootorder($newboLegacy, $AuthorizationToken)`. La variable `$AuthorizationToken` permet de transmettre le mot de passe du BIOS.

5. Modification de la séquence d'amorçage de la liste d'amorçage type 2 en utilisant PowerShell :
   a. Obtenez la séquence d'amorçage actuelle de la liste d'amorçage type 2 en exécutant la commande suivante : `$boUefi = Get-WmiObject -namespace root\dcim\sysman -class dcim_orderedcomponent | where {$_.partcomponent -match 'BootListType-2'} | select -expand partcomponent.`
   b. Définissez une variable PowerShell pour spécifier la séquence d'amorçage pour définir `$newboUefi`. Attribuez-lui la nouvelle séquence d'amorçage. Par exemple, la séquence d'amorçage actuelle est conservée.
   c. Obtenez l'instance `dcim_bootconfigsetting` correspondant à la liste d'amorçage type 2 en exécutant la commande suivante : `$bcsUefi = Get-WmiObject -Namespace root\dcim\sysman -ClassName dcim_bootconfigsetting | where {$_.ElementName -eq 'Next Boot Configuration Setting : Boot List Type 2'}.`
   d. Lancez la méthode en exécutant la commande suivante : `$ bcsUefi.changebootorder($newboUefi, $AuthorizationToken)`. La variable `$AuthorizationToken` permet de transmettre le mot de passe du BIOS.

Arrêt et redémarrage à distance du système Windows

Vous pouvez arrêter ou redémarrer le système Windows à distance à l'aide de la méthode RequestStateChange.

1. Arrêtez le système Windows à distance à l'aide de la commande suivante :

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

2. Redémarrez le système Windows à distance à l'aide de la commande suivante :

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

Obtention à distance de la valeur temporelle du système sur système Windows

Vous pouvez obtenir la valeur temporelle du système Windows à distance à l'aide de la méthode ManageTime. Par exemple :

Dans l'interface de ligne de commande, exécutez la commande suivante :

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

Gestion locale des systèmes clients Dell à l'aide de Dell Command | Monitor 10.6

Vous pouvez gérer les systèmes clients Dell localement en utilisant les méthodes suivantes :

- Pour les systèmes exécutant Windows, à l'aide de PowerShell
- Pour les systèmes exécutant Linux, à l'aide d'OMICLI

Sujets :

Gestion locale de systèmes Windows en utilisant PowerShell

Vous pouvez gérer les systèmes clients Dell en exécutant Windows en local à l'aide de commandes PowerShell.

- Énumération des instances d'une classe DCIM
  - `Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSEnumeration`
  - `Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSPassword`
- Obtention de propriétés pour les paramètres du BIOS

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

- Modification des paramètres du BIOS

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

- Modification des valeurs non critiques

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

- Abonnement à des alertes

```
$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)
```

- Commandes pour obtenir le consentement de l'utilisateur de WMI :

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

- Commandes pour définir le consentement de l'utilisateur à partir de WMI :

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

REMARQUE : Le programme d'amélioration est disponible pour Dell Command | Monitor version 10.5 et 10.6 x64 bits.

- Commandes pour obtenir le proxy à partir de WMI :

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

- Commandes pour définir le proxy à partir de WMI :

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

Gestion locale de systèmes Linux en utilisant OMICLI

Vous pouvez gérer les systèmes Linux localement à l'aide des commandes OMICLI. Sur les systèmes exécutant Linux, OMICLI est installé sous `/opt/omi/bin`.

- Énumération des instances d'une classe DCIM
  - `./omicli ei root/dcim/sysman DCIM_BIOSEnumeration`
  - `./omicli ei root/dcim/sysman DCIM_BIOSPassword`
- Obtention de propriétés pour les paramètres du BIOS

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

- Définition du mot de passe de l'administrateur

```
./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 }
```

- Modification des paramètres du 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> }
```

- Abonnement à des alertes

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

7

Gestion à distance des systèmes clients Dell à l'aide de Dell Command | Monitor 10.6

Vous pouvez gérer les systèmes clients Dell à distance en utilisant l'une des méthodes suivantes :

- Pour les systèmes exécutant Windows, Gestion à distance de système Windows via le système Windows à l'aide de PowerShell , page 25
- Pour les systèmes exécutant Linux, Gestion à distance de systèmes Linux via le système Windows en utilisant WinRM , page 25

Sujets :

Gestion à distance de système Windows via le système Windows à l'aide de PowerShell

Vous pouvez accéder au système Windows et le surveiller à distance via le système Windows à l'aide de PowerShell.

Conditions préalables pour la gestion du système Windows :

- Windows PowerShell 3.0
- PowerShell configuré pour l'exécution de scripts distants

Conditions préalables pour le système Windows géré :

- Dell Command | Monitor
- Windows PowerShell 3.0
- PowerShell configuré pour l'exécution de scripts distants
- La fonctionnalité d'accès à distance de PowerShell doit être activée

REMARQUE :

Pour utiliser Windows PowerShell à distance, l'ordinateur distant doit être configuré pour la gestion à distance. Pour plus d'informations, dont les instructions, exécutez la commande PowerShell – `Get-Help` about_remote_requirements.

Gestion à distance de systèmes Linux via le système Windows en utilisant WinRM

Vous pouvez accéder au système exécutant Linux et le surveiller via le système exécutant Windows à l'aide des commandes WinRM.

Conditions préalables pour le système Windows

- Système d'exploitation Windows pris en charge
- Services WinRM en cours d'exécution et configurés pour la gestion à distance

Conditions préalables pour le système Linux

- Privilèges root
- Dell Command | Monitor
- Système d'exploitation Linux pris en charge
- Activer les ports 5985 et 5986 sur le serveur WMI
- Système configuré pour votre environnement

Dans l'interface de ligne de commande, exécutez

```
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
```

Gestion à distance de systèmes Linux via un système Linux à l'aide de WSMan

Vous pouvez accéder au système exécutant Linux et le surveiller à distance via le système exécutant Linux à l'aide des commandes WSMan.

Conditions préalables pour la gestion du système Linux :

- Le package de système d'exploitation Linux pris en charge est installé
- Le package wsmancli est installé

Conditions préalables pour le système Linux géré :

- Privilèges d'accès root
- Système d'exploitation Linux pris en charge
- Dell Command | Monitor

Lancez un terminal, puis exécutez

```
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

Questions fréquentes Dell Command | Monitor 10.6

- Comment trouver l'ordre (séquence) d'amorçage de la configuration d'amorçage à l'aide de la propriété DCIM_OrderedComponent.AssignedSequence ?

  Si une instance **DCIM_BootConfigSetting** (hérité ou UEFI) comporte plusieurs instances **DCIM_BootSourceSetting** (appareils d'amorçage) associées via des instances de l'association **DCIM_OrderedComponent**, la valeur de la propriété **DCIM_OrderedComponent.AssignedSequence** permet de déterminer l'ordre d'utilisation des instances **DCIM_BootSourceSetting** (appareils d'amorçage) durant l'amorçage. Un **DCIM_BootSourceSetting** dont la propriété **CIM_OrderedComponent.AssignedSequence** associée est égale à **0** est ignoré et n'est pas considéré comme inclus à la séquence d'amorçage.

- Comment modifier la séquence d'amorçage ?

  La séquence d'amorçage peut être modifiée en utilisant la méthode **DCIM_BootConfigSetting.ChangeBootOrder()**. La méthode **ChangeBootOrder()** définit l'ordre dans lequel les instances de **DCIM_BootSourceSetting** sont associées à une instance **DCIM_BootConfigSetting**. La méthode contient un paramètre d'entrée ; **Source**. Le paramètre **Source**est une baie ordonnée de la propriété **PartComponent** de la classe **DCIM_OrderedComponent** qui représente l'association entre les instances **DCIM_BootSourceSetting** (appareils d'amorçage) et l'instance **DCIM_BootConfigSetting** (type de liste de démarrage : hérité ou UEFI).

- Comment désactiver les appareils d'amorçage ?

  Lors de la modification de la séquence de démarrage, la valeur de la propriété **AssignedSequence** de chaque instance de **DCIM_OrderedComponent**, qui associe l'instance cible **DCIM_BootConfigSetting** à une instance **DCIM_BootSourceSetting** qui n'est pas présente dans la baie d'entrée du paramètre **Source**, est définie sur **0**, indiquant que le périphérique est désactivé.

- Le message d'échec de connexion s'affiche lorsque <appareil/profil tentant de se connecter> tente de se connecter à l'espace de nommage avec wbemtest.

  Lancez **wbemtest** avec des privilèges d'administration pour éviter les messages de connexion. Accédez à Internet Explorer dans la liste **Tous les programmes**, cliquez avec le bouton droit de la souris et sur **Exécuter en tant qu'administrateur** pour lancer **wbemtest** et éviter les erreurs liées à l'espace de nommage.

- Comment exécuter des scripts de la bibliothèque de connaissances sans problème ?

  Voici les étapes à suivre pour exécuter les scripts VBS fournis dans le lien de la bibliothèque de connaissances Dell Command | Monitor :

  1. Configurez **winrm** sur le système en exécutant la commande `winrm quickconfig`.
  2. Vérifiez que la prise en charge des jetons existe sur le système en consultant :
     - L'**écran F2** dans la configuration du BIOS.
     - Utilisez un outil tel que wbemtest pour vérifier que les valeurs clés sont définies dans le script pour exister dans le système.

     REMARQUE : Dell recommande d'utiliser la version la plus récente du BIOS disponible à l'adresse **dell.com/support**. Pour en savoir plus, voir le Guide de référence de Dell Command | Monitor sur **dell.com/support**.

- Comment puis-je définir les attributs BIOS ?

  Les attributs du BIOS peuvent être modifiés en utilisant la méthode **DCIM_BIOSService.SetBIOSAttributes()**. La méthode **SetBIOSAttributes()** définit la valeur de l'instance définie dans la classe **DCIM_BIOSEnumeration**. La méthode comporte sept paramètres d'entrée. Les deux premiers paramètres peuvent être vides ou NULL. Le troisième paramètre **AttributeName** doit faire passer l'adressage d'entrée à la valeur de l'instance de la classe **DCIM_BIOSEnumeration**. Le quatrième paramètre ou **AttributeValue** peut être toute valeur possible du nom d'attribut tel que défini dans **DCIM_BIOSEnumeration**. Le cinquième paramètre AuthorizationToken est facultatif. L'entrée du cinquième paramètre est le mot de passe du BIOS. Le cinquième paramètre n'est utilisé que lorsque le mot de passe du BIOS est défini sur le système, sinon il est vide. Les sixième et septième arguments peuvent également être vides ou NULL

- Dell Command | Monitor prend-il en charge la surveillance du stockage et des capteurs pour les systèmes d'exploitation Windows et Linux ?

Oui, Dell Command | Monitor prend en charge à la fois la surveillance du stockage et des capteurs pour les systèmes d'exploitation Windows et Linux pris en charge.

Concernant la surveillance du stockage, Dell Command | Monitor prend en charge la surveillance et les alertes issues de :

- Contrôleur intégré Intel (conforme à CSMI v0.81 ou version ultérieure)
- Contrôleurs RAID intégrés LSI ; et 9217, 9271, 9341, 9361 et leurs pilotes associés (physiques et logiques)

REMARQUE : La surveillance de contrôleur intégré Intel n'est pas prise en charge sur les systèmes exécutant le système d'exploitation Linux.

Concernant la surveillance des capteurs, Dell Command | Monitor prend en charge la surveillance et les alertes de la tension, de la température, de l'ampérage, des périphériques de refroidissement (ventilateur) et des capteurs du châssis.

Pour plus d'informations sur les classes et les alertes, consultez le Guide de référence Dell Command | Monitor sur **dell.com/support**.

- Dell Command | Monitor peut-il être intégré à d'autres applications/consoles ?

  Oui, les interfaces Dell Command | Monitor peuvent être associées aux principales consoles de gestion d'entreprise qui prennent en charge les normes du secteur. Il peut être intégré aux outils de gestion d'entreprise suivants :

  - Dell Client Integration Suite for System Center 2012
  - Dell OpenManage Essentials
  - Dell Client Management Pack for System Center Operation Manager
- Puis-je importer des classes dans SCCM pour inventaire ?

  Oui, des classes MOF individuelles ou des fichiers OMCI_SMS_DEF.mof peuvent être importés dans la console SCCM pour inventaire.
- Où se trouve le fichier SCCM OMCI_SMS_DEF.mof ?

  Le fichier OMCI_SMS_DEF.mof se trouve dans C:\Program Files\Dell\Command_Monitor\ssa\omacim\OMCI_SMS_DEF.mof.
- Comment configurer le proxy pour DCM 10.2.1 ?
- DCM 10.2.1 ne parvient pas à récupérer les informations sur la garantie.
- Vérifiez que les paramètres de proxy de l'application sont correctement configurés à l'aide de la classe DCIM_ApplicationProxySetting.

  Comment puis-je configurer les informations d'identification de proxy pour Dell Command | Monitor ?

  Si vous vous êtes connecté via Dell Command | Monitor, vous pouvez utiliser les mêmes informations d'identification pour l'authentification du proxy.
- Dell Command | Monitor n'affiche pas les informations de garantie.
  - Le système client n'est pas connecté à Internet lors de l'interrogation.

    Connectez-vous à Internet et consultez les informations de garantie en exécutant la commande suivante `Get-CimInstance -Namespace root/DCIM/SYSMAN -ClassName DCIM_AssetWarrantyInformation| Where-Object{$_.InstanceID -eq "Root/MainSystemChassis/COOObject/COOWarranty:0"} | Invoke-CimMethod -MethodName RefreshWarranty`
  - Le système client n'est pas configuré avec le serveur proxy.

    Configurez les paramètres du proxy dans Dell Command | Monitor en exécutant les commandes suivantes :

    - Pour obtenir le proxy à partir de WMI, exécutez la commande suivante `Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_ApplicationProxySetting` :
    - Pour configurer le proxy à partir de WMI, exécutez la commande suivante : `Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_ApplicationProxySetting | Invoke-CimMethod -MethodName Change ProxySetting -Arguments @{NewAddress="10.0.0.223"; NewPort="8080"}`

      Vous devez remplacer la **Nouvelle Adresse** et le **Nouveau Port** en fonction de l'environnement proxy (le cas échéant).

9

Étapes de dépannage à l'aide de Dell Command | Monitor 10.6

Sujets :

Impossible de se connecter à distance à Windows Management Instrumentation

Si l'application de gestion ne peut pas obtenir les informations CIM (Common Information Model) d'un système informatique client à distance ou si la mise à jour à distance du BIOS, qui utilise un modèle DCOM (Distributed Component Object Model), échoue, les messages d'erreur suivants s'affichent :

- **Accès refusé.**
- **Win32 : le serveur RPC n'est pas disponible**

1. Vérifiez que le système client est connecté au réseau. Entrez la commande suivante dans l'invite de commande du serveur : `ping <Host Name or IP Address>` et appuyez sur `<Enter>`.
2. Effectuez les étapes suivantes si le serveur et le système client se trouvent dans le même domaine :
   - Vérifiez que le compte administrateur du domaine a des droits d'administrateur pour les deux systèmes.

   Effectuez les étapes suivantes si le serveur et le système client se trouvent dans un groupe de travail (et pas dans le même domaine) :
   - Assurez-vous que le serveur est en cours d'exécution sur le serveur Windows le plus récent.

   REMARQUE : Avant de modifier le registre, sauvegardez vos fichiers de données système. Si vous effectuez des modifications incorrectes dans le registre, le système d'exploitation peut devenir inutilisable.
3. Modifiez le registre sur le système client. Cliquez sur **Démarrer** > **Exécuter**, entrez **regedit,**, puis cliquez sur **OK**. Dans la fenêtre de l'**Éditeur de registre**, accédez à My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa.
4. Définissez la valeur de **forceguest** sur 0 (la valeur par défaut est 1). Sauf si vous modifiez cette valeur, l'utilisateur qui se connecte à distance au système obtient des privilèges d'invité, même si les informations d'identification qu'il fournit accordent des privilèges d'administration.
   a. Créez un compte sur le système client avec le même nom d'utilisateur et le même mot de passe qu'un compte administrateur sur le système exécutant l'application de gestion WMI.
   b. Si vous utilisez IT Assistant, exécutez son utilitaire ConfigServices (configservices.exe situé dans le répertoire /bin du répertoire d'installation IT Assistant). Configurez IT Assistant pour l'exécuter sous un compte administrateur local, qui maintenant est également administrateur sur le client à distance. Vérifiez également que DCOM et CIM sont activés.
   c. Si vous utilisez IT Assistant, utilisez le compte administrateur pour configurer la détection de sous-réseaux sur le système client. Saisissez le nom d'utilisateur sous la forme <nom de la machine client>\<nom du compte>. Si le système a déjà été détecté, supprimez-le de la liste de systèmes détectés, configurez la détection des sous-réseaux, puis exécutez à nouveau la détection.

   REMARQUE : Dell vous conseille d'utiliser Dell OpenManage Essentials à la place d'IT Assistant. Pour plus d'informations sur Dell OpenManage Essentials, consultez la page **dell.com/support**.
5. Procédez comme suit pour modifier les niveaux de privilège utilisateur pour vous connecter à distance aux services WMI d'un système :
   a. Cliquez sur **Démarrer** > **Exécuter**, entrez `compmgmt.msc`, puis cliquez sur **OK**.

b. Naviguez vers **Contrôle WMI** sous **Services et applications**.
c. Cliquez avec le bouton droit sur **Contrôle WMI**, puis cliquez sur **Propriétés**.
d. Cliquez sur l'onglet **Sécurité**, puis sélectionnez **DCIM/SYSMAN** sous l'arborescence **Racine**.
e. Cliquez sur **Sécurité**.
f. Sélectionnez le groupe ou l'utilisateur spécifique dont vous souhaitez contrôler l'accès et utilisez la case à cocher **Autoriser** ou **Refuser** pour configurer les autorisations.

6. Effectuez les étapes suivantes pour vous connecter à l'infrastructure WMI (root\DCIM/SYSMAN) sur un système à partir d'un système distant en utilisant WMI CIM Studio :
   a. Installez les outils WMI et wbemtest sur le système local, puis installez Dell Command | Monitor sur le système distant.
   b. Configurez le pare-feu sur le système pour la connectivité à distance WMI. Par exemple, ouvrez les ports TCP 135 et 445 dans le pare-feu Windows.
   c. Définissez le paramètre Sécurité locale sur **Classique : les utilisateurs locaux s'authentifient eux-mêmes pour Accès réseau : modèle de partage et de sécurité pour les comptes locaux** dans la **Stratégie de sécurité locale**.
   d. Connectez-vous à l'infrastructure WMI (root\DCIM\SYSMAN) sur le système local à partir d'un système distant en utilisant WMI wbemtest. Par exemple, \\[Adresse IP du système distant cible]\root\DCIM\SYSMAN
   e. Entrez les informations d'identification de l'administrateur du système distant cible si vous êtes invité à le faire.

   Pour en savoir plus sur WMI, consultez la documentation Microsoft appropriée sur msdn.microsoft.com.

Échec de l'installation sur les systèmes exécutant Windows

Si vous ne parvenez pas à réaliser l'installation de Dell Command | Monitor pour Windows, assurez-vous que :

- Vous détenez des privilèges d'administrateur sur le système cible.
- Le système cible est un système élaboré Dell avec SMBIOS version 2.3 ou ultérieure.
- La console PowerShell ne doit pas être ouverte.

REMARQUE : Pour vérifier la version du SMBIOS du système, accédez à **Démarrer** > **Exécuter**, exécutez le fichier `msinfo32.exe`, puis recherchez la version du SMBIOS dans la page Récapitulatif du système.

REMARQUE : Le système doit exécuter le système d'exploitation Windows pris en charge.

REMARQUE : Le système doit être mis à niveau à .NET 4.0 ou versions ultérieures.

La valeur d'énumération du paramètre du BIOS est 1

1. Assurez-vous que les packages suivants sont installés avec des privilèges d'utilisateur 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. Si les packages ci-dessus sont installés, assurez-vous que le module du pilote est chargé.
   a. Assurez-vous que le module du pilote est chargé en exécutant la commande suivante : `lsmod | grep dcdbas`.
   b. Si le module du pilote n'est pas disponible, récupérez les informations du pilote en exécutant la commande suivante : `modinfo dcdbus`.
   c. Lancez le module du pilote en exécutant la commande suivante : `insmod <filename>`.

L'installation d'Hapi échoue à cause de la dépendance de libsmbios

Si l'installation échoue à cause de problèmes de dépendance,

forcez l'installation de tous les packages dépendants en exécutant la commande `apt-get -f install`.

Ressources CIM non disponibles

Lors de l'énumération, si vous recevez un message d'erreur tel que « CIM resource not available », vérifiez que les commandes sont exécutées avec des privilèges root.

Impossible d'exécuter les commandes à l'aide de DCM sur les systèmes exécutant Ubuntu Core 16

Assurez-vous que la version snapshot sur le système est 2.23 ou une version ultérieure.

10

Autres documents utiles

En plus de ce Guide de l'utilisateur, vous pouvez accéder aux documents suivants sur **dell.com/support**. Cliquez sur Dell Command | Monitor (anciennement OpenManage Client Instrumentation), puis sur le lien de la version du produit appropriée dans la section **Support général**.

En plus de ce Guide de l'utilisateur, vous pouvez accéder aux guides suivants :

- Le Guide de référence de Dell Command | Monitor fournit des informations détaillées sur toutes les classes, propriétés et descriptions.
- Le Guide d'installation de Dell Command | Monitor fournit des informations sur l'installation.
- Le Guide de référence SNMP de Dell Command | Monitor fournit Simple Network Management Protocol (SNMP) Management Information Base (MIB) applicable à Dell Command | Monitor.

Sujets :

Accès aux documents à partir du site de support Dell

Vous pouvez accéder aux documents requis en sélectionnant votre produit.

1. Rendez-vous sur www.dell.com/manuals.
2. Cliquez sur **Parcourir tous les produits**, puis sur **Logiciel** et enfin sur **Gestion des systèmes clients**.
3. Pour afficher les documents requis, cliquez sur le nom et le numéro de version du produit requis.

11

Contacter Dell

REMARQUE : Si vous ne possédez pas une connexion Internet active, vous pourrez trouver les coordonnées sur votre facture d'achat, bordereau d'expédition, acte de vente ou catalogue de produits Dell.

Dell offre plusieurs options de service et de support en ligne et par téléphone. La disponibilité des produits varie selon le pays et le produit. Certains services peuvent ne pas être disponibles dans votre région. Pour contacter le service commercial, du support technique ou client de Dell :

1. Rendez-vous sur **Dell.com/support**.
2. Sélectionnez la catégorie de support
3. Recherchez votre pays ou région dans le menu déroulant **Choisissez un pays ou une région** situé au bas de la page.
4. Sélectionnez le lien de service ou de support en fonction de vos besoins.