Dell Command | Monitor Version 9.2.1
Guide d’utilisation

Remarques, précautions et avertissements

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

PRÉCAUTION : Une PRÉCAUTION indique un risque d'endommagement du matériel ou de perte de données et vous indique comment éviter le problème.

AVERTISSEMENT : Un AVERTISSEMENT indique un risque d'endommagement du matériel, de blessures corporelles ou même de mort.

2017 - 05

Rév. A00

Table des matières

1

Introduction

L'application du Dell Command | Monitor logiciel permet la gestion à distance à l'aide de programmes d'application pour accéder aux informations, surveiller l'état ou modifier l'état du système, tel que l'arrêt à distance du système. Dell Command | Monitor Utilise des paramètres clés du système par l'intermédiaire d'interfaces standard qui permettent aux administrateurs de gérer l'inventaire, de surveiller l'intégrité du système et de rassembler des informations sur les systèmes Dell déployés. Dell Command | Monitor est conçu pour les systèmes clients Dell Enterprise, les systèmes Dell IoT Gateway, ainsi que pour les Dell Embedded PC. Pour plus d'informations sur les systèmes Dell pris en charge reportez-vous aux Notes de mise à jour, disponibles sur **dell.com/dellclientcommandsuitemanuals**. Ce document donne une vue d'ensemble de Dell Command | Monitor et de ses fonctionnalités.

REMARQUE : Dell Command | Monitor était connu précédemment sous le nom Dell OpenManage Client Instrumentation (OMCI). Après la sortie de la version OMCI 8.2, OMCI a été renommé Dell Command | Monitor.

Nouveautés de cette version

- Prise en charge d'une nouvelle plateforme : Dell Edge Gateway série 3000
- Prise en charge du nouveau système d'exploitation : Ubuntu Core 16
- Prise en charge des nouveaux paramètres du BIOS suivants :
  - Mode d'interface analogique et numérique canal 1
  - Mode d'interface analogique et numérique canal 2
  - Mode d'interface analogique et numérique canal 3
  - Mode d'interface analogique et numérique canal 4
  - Mode d'interface analogique et numérique canal 5
  - Mode d'interface analogique et numérique canal 6
  - Mode d'interface analogique et numérique canal 7
  - Mode d'interface analogique et numérique canal 8
  - Période de réveil automatique
  - Effacer le journal du BIOS
  - Effacer le journal d'alimentation
  - Effacer le journal thermique
  - Capteurs MEM
  - ZigBee

Pour en savoir plus sur les jetons, voir le *Guide de référence Dell Command | Monitor* sur **dell.com/dellclientcommandsuitemanuals**.

Présentation de Dell Command | Monitor

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 en appliquant le modèle CIM (Common Information Model) et le protocole SNMP (Simple Network Management Protocol), qui sont des protocoles de gestion. Cela réduit le coût total de possession, renforce la sécurité et fournit une approche globale à la gestion de tous les appareils d'un réseau, notamment : systèmes clients, serveurs, systèmes de stockage, systèmes de gestion de réseau et dispositifs logiciels.

Le modèle CIM vous permet d'accéder à Dell Command | Monitor via les standards de gestion 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, notamment : du BIOS, du CMOS, du SMBIOS (System Management BIOS), de l'interface SMI (System Management Interface), du système d'exploitation et des API (Application Programming Interface). Dell Command Monitor pour Windows collecte également des informations relatives aux bibliothèques de liens dynamiques (DLL) et aux paramètres de registre. Pour Windows, Dell Command | Monitor récupère ces informations via l'interface CIMOM (CIM Object Manager), la pile WMI (Windows Management Instrumentation) ou l'agent SNMP. Pour Linux, l'application récupère ces informations via l'interface OMI (Open Management Infrastructure).

Dell Command | Monitor permet aux administrateurs informatiques de collecter à distance des informations sur les actifs, de modifier les paramètres du BIOS, de recevoir des notifications proactives en cas de risques de pannes et des alertes en cas d'atteinte à la sécurité. Sur les systèmes exécutant Windows, ces alertes sont disponibles sous forme d'événements dans le journal d'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 implémenté l'intégration 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 Dell TechCenter, 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, voir le *Guide d'installation Dell Command | Monitor* sur dell.com/dellclientcommandsuitemanuals.

2

Fonctionnalités

Principales fonctionnalités de l'outil Dell Command | Monitor :

- Prise en charge du schéma CIM
- Configuration du BIOS
- Sécurité WMI/OMI
- Rapport d'événements
- Arrêt à distance
- Accès aux informations système en utilisant le schéma CIM et le protocole WSMAN

  REMARQUE : L'outil Dell Command | Monitor pour Windows permet également d'accéder aux informations en utilisant le protocole SNMP.
- Compilation des informations d'inventaire détaillées
- Possibilité de configuration de réveil à distance
- Modification à distance des paramètres système
- Contrôle de l'intégrité du système et de l'état des rapports
- Surveillance et alertes RAID pour les contrôleurs intégrés Intel et LSI.

  REMARQUE : La surveillance de contrôleur intégré Intel n'est pas prise en charge sur les systèmes exécutant le système d'exploitation Linux.
- Surveillance et interruptions SNMP uniquement en utilisant Dell Command | Monitor pour Windows

Prise en charge du schéma CIM

Dell Command | Monitor pour Windows est conforme au schéma CIM 2.17, et il inclut deux fournisseurs WMI :

- Fournisseur d'indications/Agent d'interrogation WMI
- Fournisseur d'instances ou méthodes WMI

Dell Command | Monitor pour Linux est conforme au schéma CIM 2.32.0, et il inclut deux fournisseurs WMI :

- Fournisseur d'indications/Agent d'interrogation WMI
- Fournisseur d'instances ou méthodes WMI

Configuration et énumération des paramètres du BIOS

Dell Command | Monitor permet de configurer le BIOS d'un système.

Sécurité WMI/OMI

WMI permet d'instaurer l'authentification utilisateur avant d'autoriser l'accès aux données et aux méthodes CIM. Les droits d'accès sont appliqués par le modèle de sécurité DCOM (Distributed Component Object Model) et le gestionnaire CIMOM. L'accès complet ou restreint est accordé aux utilisateurs en fonction des espaces de noms. Aucune sécurité n'est implémentée au niveau des classes ou des propriétés. Par défaut, les utilisateurs membres du groupe d'administrateurs ont l'accès complet local et distant à WMI.

Avec Dell Command | Monitor pour Windows, vous pouvez configurer la sécurité WMI en utilisant le contrôle WMI disponible sur la console Gestion de l'ordinateur dans la section Services et Applications. Cliquez avec le bouton droit sur **Contrôle WMI**, puis cliquez

sur **Propriétés**. Vous pouvez configurer la sécurité spécifique aux espaces de noms dans l'onglet **Sécurité**. Vous pouvez également exécuter le **Contrôle WMI** depuis le menu **Démarrer** ou via l'interface **CLI**, en exécutant `wmimgmt.msc`.

Rapports d'alertes

Dell Command | Monitor détecte les événements sur les systèmes Dell et informe l'utilisateur local et l'administrateur de réseau, notamment sur les risques de panne, les modifications de configuration, l'inventaire des composants, les contrôleurs RAID Intel et LSI intégrés, les capteurs et les intrusions dans le châssis. Ces événements sont affichés par une application de gestion des systèmes, telle qu'OME (OpenManage Essentials).

Arrêt à distance

Dell Command | Monitor pour Windows prend en charge l'arrêt et le redémarrage du système à distance.

Accès aux informations du système

Dell Command | Monitor permet d'accéder aux informations système telles que la version du BIOS, le fabricant ou fournisseur du BIOS, le numéro de série, la date du premier démarrage et le modèle de système via WMI/OMI en utilisant le gestionnaire CIM. Le protocole WSMAN peut également permettre d'accéder à ces informations via WMI/OMI.

Informations d'inventaire détaillées

Dell Command | Monitor donne accès à des informations détaillées, notamment sur les processeurs, la mémoire, les dispositifs PCI et les batteries.

Configuration des paramètres de réveil à distance

Dell Command | Monitor prend en charge la configuration des paramètres de réveil à distance. Le réveil à distance est une fonction du système client et de la carte d'interface réseau (NIC).

Modification à distance des paramètres du BIOS du système

Dell Command | Monitor permet aux administrateurs de récupérer et de configurer les paramètres du BIOS des systèmes clients d'entreprise, notamment la configuration des ports USB, les paramètres de la carte d'interface réseau, etc.

État et intégrité du système

Dell Command | Monitor contrôle l'intégrité du système et fournit l'état des composants tels que le ventilateur, la mémoire, la température, les capteurs, la batterie, les contrôleurs RAID, la station d'accueil.

Surveillance et alertes RAID pour les contrôleurs Intel et LSI

Surveillance et alertes pour les contrôleurs RAID Intel et LSI, les lecteurs logiques et physiques avec Dell Command | Monitor pour Windows. Surveillance et alertes uniquement pour les contrôleurs LSI avec Dell Command | Monitor pour Linux.

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)

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

- Contrôleurs RAID intégrés LSI ; et 9217, 9271, 9341, 9361 et leurs pilotes associés (physiques et logiques)

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

Surveillance et interruptions SNMP

Dell Command | Monitor pour Windows est conforme à la norme SNMP v1 et prend en charge la surveillance des attributs et interruptions du système.

3

Standards et protocoles

Dell Command | Monitor est basé sur les standards CIM. La spécification CIM décrit des techniques d'adressage permettant d'améliorer la compatibilité avec les protocoles de gestion.

Les 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 standards reconnu dans le secteur qui dirige le développement, l'adoption et l'unification des standards de gestion (notamment CIM et ASF) et les initiatives pour les environnements de bureau, d'entreprise et Internet.

4

Scénarios d'utilisation

Ce chapitre décrit les divers scénarios d'utilisation de l'outil Dell Command | Monitor.

Vous pouvez utiliser Dell Command | Monitor pour :

- Gestion de l'inventaire
- Gestion des configurations
- Surveillance de l'intégrité
- Profils

Scénario 1 : Gestion de l'inventaire

Une société utilisant de nombreux systèmes Dell ne parvient pas à gérer de façon précise les informations d'inventaire en raison de changements dans les équipes commerciale et informatique. Le directeur informatique demande un plan d'identification des systèmes qui peuvent être mis à niveau vers les dernières versions de Microsoft Windows. Cela requiert l'évaluation des systèmes déployés pour déterminer la taille, l'étendue et l'impact financier d'un tel projet. La collecte d'informations est une tâche considérable. Le déplacement d'un technicien informatique sur chaque système client coûte cher en termes d'heures de travail et d'interruptions pour les utilisateurs.

Si Dell Command | Monitor est installé sur les systèmes Dell, le responsable informatique peut rapidement collecter des informations à distance. À l'aide d'outils tels que le gestionnaire SCCM (Microsoft System Center Configuration Manager), le responsable informatique peut interroger chaque système client via le réseau et collecter des informations telles que le type et la vitesse des processeurs, la taille de la mémoire, la capacité du disque dur, la version du BIOS et la version du système d'exploitation. L'analyse des informations collectées permet ensuite d'identifier les systèmes qu'il est possible de mettre à niveau vers les dernières versions de Windows.

Vous pouvez également obtenir l'inventaire des actifs en utilisant la ligne de commande WSMAN/WinRM ou une ligne de commande CIM.

Intégration SCCM

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

- En utilisant le fichier MOF inclus au package d'installation Dell Command | Monitor, qui contient toutes les classes Dell Command | Monitor, et en l'important dans ConfigMgr.

  Le fichier MOF se trouve à l'emplacement suivant :

  C:\Program Files\Dell\Command_Monitor\ssa\omacim\OMCI_SMS_DEF.mof
- En étendant 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 achète une suite d'outils, puis prévoit d'automatiser le déploiement d'un nouveau système d'exploitation client en utilisant l'environnement de pré-amorçage PXE (Preboot Execution Environment).

Le défi consiste à trouver un moyen de modifier à distance le mot de passe du BIOS de chaque poste de travail. Si Dell Command | Monitor est installé sur chaque système client, l'équipe informatique de la société dispose de différentes options pour modifier la

séquence d'amorçage. La console de gestion OME (OpenManage Essentials) peut être intégrée à Dell Command | Monitor et utilisée pour surveiller les paramètres du BIOS à distance sur tous les systèmes clients de l'entreprise. 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, voir le *Guide de référence Dell Command | Monitor* sur **dell.com/dellclientcommandsuitemanuals**.

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. Si Dell Command | Monitor est installé sur chaque système client, le département informatique peut verrouiller les ports hérités pour éviter l'utilisation de périphériques non autorisés, ou activer la fonction Wake On LAN (WOL) pour que le système sorte du mode veille durant les heures creuses afin d'exécuter des tâches de gestion.

Scénario 3 : Surveillance de l'intégrité

Un utilisateur reçoit des messages d'erreur de lecture lorsqu'il tente d'accéder à certains fichiers sur le disque dur du système client. L'utilisateur redémarre le système et les fichiers semblent maintenant être accessibles. L'utilisateur ignore le problème initial car il semble s'être résolu sans intervention. Pendant ce temps, Dell Command | Monitor interroge le disque dur pour lequel le problème se pose pour trouver un échec prévu et envoie une alerte SMART (Self-Monitoring , Analysis and Reporting Technology) à la console de gestion. Il affiche également l'erreur SMART à l'utilisateur local. L'alerte indique que le disque dur est affecté de plusieurs erreurs de lecture/écriture. Le service informatique de la société recommande à l'utilisateur d'effectuer immédiatement une sauvegarde des fichiers de données essentiels. Un technicien de maintenance est envoyé avec un lecteur de rechange.

Le disque dur est remplacé avant de tomber en panne, ce qui prévient tout temps de non-fonctionnement, un appel au service d'aide et le déplacement d'un technicien en vue de diagnostiquer le problème.

Surveillance 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 via les 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, voir le *Guide de référence Dell Command | Monitor* sur **dell.com/dellclientcommandsuitemanuals**.

Scénario 4 : Profils

REMARQUE : Les profils DMTF sont mis en œuvre 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 difficultés et représenter les données de gestion fournies, les profils DMTF (Distributed Management Task Force) et DCIM-OEM (Data Center Infrastructure Management) sont implémentés dans Dell Command | Monitor. Certains profils DMTF sont expliqués dans ce guide.

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

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**.

Profil de gestion du BIOS

- Déterminez la version du BIOS en énumérant l'instance de la classe **DCIM_BIOSElement.Version**.
- Vérifiez si 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.SetBIOSAttribute()** et définissez le SystemPwd sur AttributeName et la valeur du mot de passe sur les paramètres AttributeValue.
- Définissez le mot de passe BIOS ou Admin (AdminPwd). Exécutez la méthode **DCIM_BIOSService.SetBIOSAttribute()** et définissez le 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 de l'amorçage

- Modifiez la séquence des éléments d'amorçage dans la liste de d'amorçage Héritée et UEFI.
- Activez ou désactivez les éléments d'amorçage dans la liste d'amorçage Héritée et UEFI.
- Trouvez la configuration de démarrage 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 de démarrage 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**.
- Exécutez la méthode **DCIM_ComputerSystem.RequestStateChange()** et définissez la valeur du paramètre RequestedState sur **3**. Mettez hors tension le système.
- Redémarrez le système. Exécutez la méthode **DCIM_ComputerSystem.RequestStateChange()** et définissez la valeur du paramètre **RequestedState** sur **11**.
- 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.
- Trouvez les entrées de journal individuelles. Obtenez toutes les instances de **DCIM_LogEntry** qui sont associées à l'instance donnée de **DCIM_RecordLog** au moyen de l'association **DCIM_LogManagesRecord**. Triez les instances en fonction du **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 journaux en fonction de l'horodatage de l'entrée de journal. Obtenez toutes les instances de **DCIM_LogEntry** qui sont associées à l'instance donnée de **DCIM_RecordLog** au moyen de l'association

DCIM_LogManagesRecord. Triez les instances de **DCIM_LogEntry** en fonction de la valeur de la propriété **CreationTimeStamp** dans l'ordre LIFO (last in first out - dernier entré premier sorti).

- 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 pièce 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

Utilisation de Dell Command | Monitor

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, voir le *Dell Command | MonitorGuide de référence* sur **dell.com/dellclientcommandsuitemanuals**.

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 de courant, l'augmentation et la réduction de la capacité du disque, l'augmentation et la réduction de mémoire, l'augmentation et la réduction du nombre de processeurs, en utilisant Dell Command | Monitor :

- Pour Windows, le fichier dcsbdy32.ini ou dcsbdy64.ini se trouve dans <Dell Command | Monitor installed location>\omsa\ini.
- Pour Linux, le fichier AlertPollingSettings.ini se trouve dans /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 capacité de disque et l'alerte SMART (Self-Monitoring, Analysis and Reporting Technology) est de 626 secondes (temps réel = 626 X 23 secondes, ce qui équivaut à environ 3 heures).

Rapport d'état RAID

Dell Command | Monitor active les informations de configuration RAID et surveille la fonctionnalité RAID sur les systèmes clients qui prennent en charge le matériel et les pilotes. Vous pouvez utiliser les classes RAID pour obtenir des informations sur les niveaux RAID, les pilotes, la configuration du contrôleur et l'état du contrôleur. Une fois la configuration RAID activée, vous pouvez recevoir des alertes concernant la dégradation ou les pannes des lecteurs et des contrôleurs.

REMARQUE : Les rapports d'état RAID sont pris en charge uniquement pour les contrôleurs RAID fonctionnant avec les pilotes conformes à CSMI (Common Storage Management Interface) version 0.81. OMCI 8.1 et versions ultérieures prennent en charge la surveillance uniquement sur le contrôleur RAID sur puce Intel, et OMCI 8.2 et version 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 utilisé à la fois par Dell Command | Monitor et par Server Administrator. Dell Command | Monitor pour Windows version 9.0 a été modifié pour utiliser un OID spécifique à l'OID client (10909) pour identifier les systèmes clients sur les consoles.

Pour plus d'informations sur le protocole SNMP, voir le *Guide de référence SNMP Dell Command | Monitor* sur **dell.com/dellclientcommandsuitemanuals**.

- Dell Command | Monitor pour Linux prend en charge la surveillance en utilisant les commandes WinRM et WSMan.

Journal d'application pour 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 dans **/opt/dell/dcm/var/log**.

Fichier de configuration

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

REMARQUE : Après avoir modifié le fichier de configuration, redémarrez le serveur OMI afin d'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 (débogage), 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 lecteurs à format avancé

Les systèmes client basculent vers des disques AF (Advanced Format - Format avancé) afin d'obtenir une capacité de stockage plus élevée et pour traiter les limites associées aux disques durs (HDD) dotés de secteurs de 512 octets. Les disques durs basculant vers les secteurs de 4 Ko conservent la rétro-compatibilité , alors que les disques durs AF actuels, aussi nommés disques durs 512e, correspondent à SATA 512 octets et fonctionnent à 4 Ko. Pendant la transition, vous risquez de rencontrer des problèmes de performances, tels que des disques de partition mal alignés, dans les systèmes clients, provoquant l'échec de logiciels de cryptage à base de secteur qui traitent 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 d'amorçage

REMARQUE : Dell Command | Monitor pour Linux ne permet pas de configurer l'amorçage. Cette section n'est donc pas applicable 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 l'amorçage (Hérité ou UEFI) est modélisée en utilisant les classes suivantes :

- **DCIM_ElementSettingData**
- **DCIM_BootConfigSetting**
- **DCIM_OrderedComponent**
- **DCIM_BootSourceSetting**

REMARQUE : Ici, les expressions « Configuration de démarrage » et « Type de liste d'amorçage » sont utilisées de façon interchangeable et transmettent la même signification représentant la configuration d'amorçage Hérité ou UEFI.

DCIM_BootConfigSetting

Une instance de **DCIM_BootConfigSetting** représente une configuration d'amorçage qui peut être utilisée lors du processus de démarrage. Sur les systèmes clients, par exemple, il peut y avoir deux types de configurations de démarrage : Hérité et UEFI. Ainsi, **DCIM_BootConfigSetting** a un maximum de deux instances à représenter, une pour Hérité et une pour 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 ou sources d'amorçage. Les propriétés de **ElementName**, **BIOSBootString** et **StructuredBootString** contiennent une chaîne qui identifie les périphériques d'amorçage. Par exemple : Floppy (Disquette), Hard Disk (Disque dur), CD/DVD, Network (Réseau), PCMCIA (association internationale pour les cartes mémoires d'ordinateurs personnels), BEV (véhicule à batterie électrique) ou USB. Selon le type de liste d'amorçage 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** aux instances de **DCIM_BootSourceSetting** représentant l'un des types de liste de démarrage (Hérité ou UEFI), auquel appartiennent les périphériques de démarrage. La propriété **GroupComponent** de **DCIM_OrderedComponent** se réfère à l'instance **DCIM_BootConfigSetting** et la propriété **PartComponent** se réfère à l'instance **DCIM_BootSourceSetting**.

Modification des paramètres système

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

- **SetBIOSAttributes** : modification de la configuration du BIOS

  REMARQUE : Dell Command | Monitor pour Linux prend actuellement en charge uniquement la méthode SetBIOSAttributes.
- **ChangeBootOrder** : modification de la configuration de démarrage
- **RequestStateChange** : arrêt et redémarrage du système
- **ManageTime** : affichage de 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.

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

Vous pouvez configurer les attributs du BIOS en utilisant la méthode SetBIOSAttributes. La procédure est expliquée dans l'exemple ci-dessous, relatif à la tâche d'activation du module TPM (Trusted Platform Module).

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 le module 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 en exécutant 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 module TPM en exécutant 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.

Configuration des attributs du BIOS sur un système exécutant Linux

Vous pouvez configurer les attributs du BIOS en utilisant l'une des méthodes suivantes :

- Utilisation de la méthode OMICLI
- Utilisation de la méthode WinRM
- Utilisation de la méthode WSMan

REMARQUE : Vérifiez que le serveur OMI est en cours d'exécution.

Configuration des attributs du BIOS en utilisant OMICLI

Vous pouvez configurer les attributs du BIOS en utilisant la méthode SetBIOSAttributes. La procédure est expliquée dans l'exemple ci-dessous, relatif à la tâche d'activation du module TPM (Trusted Platform Module).

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 BIOS du système s'il n'est pas 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, utilisez 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 en utilisant WinRM

Vous pouvez configurer les attributs du BIOS en utilisant la méthode SetBIOSAttributes. La procédure est expliquée dans l'exemple ci-dessous, relatif à la tâche d'activation du module TPM (Trusted Platform Module). Pour plus d'informations, voir Gestion à distance de systèmes clients Dell.

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. Récupérez le réglage du sélecteur en énumérant la classe DCIM_BIOSService. Exécutez :

   ```
   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 du sélecteur (SystemName=<nom système de classe DCIM_BIOSService>winrm i SetBIOSAttributes wsman/DCIM_BIOSService?SystemName=dt: +SystemCreationClassName=DCIM_ComputerSystem+Name=DCIM:BiosService +CreationClassName=DCIM_BIOSService+) seront utilisées pour configurer l'opération Set dans cet exemple.

2. Si le mot de passe du BIOS n'est pas défini sur le système, définissez-le en utilisant 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 module 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
   Activation");AttributeValue=("2");AuthorizationToken="<Admin password>"}
   ```

Configuration des attributs du BIOS en utilisant WSMan

Vous pouvez configurer les attributs du BIOS sur les systèmes exécutant Linux en utilisant WSMan. La procédure est expliquée dans l'exemple ci-dessous, relatif à la tâche d'activation du module TPM (Trusted Platform Module). Pour plus d'informations, voir Gestion à distance de systèmes clients Dell.

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. Récupérez le réglage du sélecteur en énumérant la classe DCIM_BIOSService. Exécutez :

   ```
   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. Si le mot de passe du BIOS n'est pas défini sur le système, définissez-le en utilisant 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 en exécutant 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 module TPM en exécutant 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 d'amorçage

Pour modifier la séquence d'amorçage, suivez les étapes suivantes :

1. Recherchez le type de liste de démarrage à l'aide de :
   - **Commande WMIC :** `wmic /namespace:\\root\dcim\sysman path dcim_BootConfigSetting get ElementName/format:list`
   - **Commande PowerShell :** `Get-CimInstace -Namespace root\dcim\sysman -ClassName DCIM_BootConfigSetting -Property ElementName`
2. Recherchez le type de commande de démarrage (hérité ou UEFI) à l'aide de :
   - **Commande WMIC :** `wmic /namespace:\\root\dcim\sysman path dcim_ElementSettingData.IsCurrent=1 get SettingData /format:list`
   - **Commande PowerShell :** `Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_ElementSettingData -Filter "IsCurrent=1" -Property SettingData`
3. Modifiez la séquence d'amorçage à l'aide de :
   - **Commande WMIC :** `wmic /namespace:\\root\dcim\sysman path dcim_bootconfigsetting call ChangeBootOrder /?:full`
   - **Commande PowerShell :** `(Get-CimClass -namespace root\dcim\sysman -ClassName DCIM_Bootconfigsetting).CimClassMethods["ChangeBootOrder"].Parameters`

   Les arguments requis pour la méthode ChangeBootOrder sont les suivants :
   - Jeton d'autorisation : il s'agit du mot de passe d'administrateur ou d'amorçage.

- Source : il s'agit de la liste de séquence d'amorçage issue de la propriété DCIM_OrderedComponent.PartComponent. La nouvelle séquence d'amorçage est déterminée par l'ordre des appareils d'amorçage dans la baie **source**.

Arrêt et redémarrage à distance d'un système Windows

Vous pouvez arrêter ou redémarrer le système Windows en utilisant la méthode RequestStateChange.

1. Arrêtez le système Windows à distance en exécutant 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 en exécutant 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 de l'heure sur un système Windows

Vous pouvez obtenir la valeur de l'heure d'un système Windows à distance en utilisant la méthode ManageTime. Par exemple :

Dans l'interface de ligne de commande, exécutez :

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 de systèmes clients Dell

Vous pouvez gérer localement des systèmes clients Dell en utilisant l'une des méthodes suivantes :

- Systèmes exécutant Windows : en utilisant PowerShell.
- Systèmes exécutant Linux : en utilisant OMICLI.

Gestion locale de systèmes Windows en utilisant PowerShell

Vous pouvez gérer localement des systèmes clients Dell exécutant Windows en utilisant des commandes PowerShell.

- **Énumération d'instances de classe DCIM**
  - `Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSEnumeration`
  - `Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSPassword`
- **Obtention des propriétés d'une configuration 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 stratégiques**

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

Gestion locale de systèmes Linux en utilisant OMICLI

Vous pouvez gérer localement des systèmes Linux en utilisant des commandes OMICLI. Sur les systèmes exécutant Linux, OMICLI est installé dans **/opt/omi/bin**.

- **Énumération d'instances de classe DCIM**
  - `./omicli ei root/dcim/sysman DCIM_BIOSEnumeration`
  - `./omicli ei root/dcim/sysman DCIM_BIOSPassword`
- **Obtention des propriétés d'une configuration BIOS**

  ```
  ./omicli gi root/dcim/sysman { DCIM_BIOSPassword InstanceID DCIM:BIOSSetupPassword }
  ```
- **Configuration du mot de passe d'administration**

  ```
  ./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 aux alertes**

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

7

Gestion à distance de systèmes clients Dell

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

- Systèmes exécutant Windows : Gestion à distance de systèmes Windows via le système Windows en utilisant PowerShell
- Systèmes exécutant Linux : Gestion à distance de systèmes Linux via le système Windows en utilisant WinRM

Gestion à distance de systèmes Windows via le système Windows en utilisant PowerShell

Vous pouvez accéder à et surveiller des systèmes Windows à distance via un système Windows en utilisant PowerShell.

Conditions requises pour le système Windows gestionnaire :

- Package du système d'exploitation Windows pris en charge installé
- Système configuré en fonction de votre environnement

Conditions requises pour le système Windows géré :

- Privilèges d'administrateur
- Dell Command | Monitor
- Package du système d'exploitation Windows pris en charge installé
- La fonction d'accès à distance PowerShell doit être activée
- Système configuré en fonction de votre environnement

1. Créez une session en ouvrant l'interface de ligne de commande et en exécutant :

   ```
   $session=New-CimSession -ComputerName "<managed system IP or system name>" -Credential
   <Administartor Credentials>
   ```
2. Entrez le mot de passe.
3. Pour accéder au système Windows et le surveiller, exécutez :

   ```
   Get-CimInstance -CimSession $session -Namespace root\dcim\sysman -ClassName <class name>
   ```

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

Vous pouvez accéder à et surveiller un système exécutant Linux via un système exécutant Microsoft Windows en utilisant des commandes WinRM.

Conditions requises sur le système Windows

- Système d'exploitation Windows pris en charge
- Services WinRM en cours d'exécution
- Système configuré pour votre environnement

Conditions requises sur le système Linux

- Privilèges root
- Dell Command | Monitor
- Système d'exploitation Linux pris en charge
- Activez 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 en utilisant WSMan

Vous pouvez accéder à et surveiller un système exécutant Linux via un système exécutant Linux en utilisant des commandes WinRM.

Conditions requises pour le système Linux de gestion :

- Package du système d'exploitation Linux pris en charge installé
- Package Wsmancli installé

Conditions requises pour le système Linux géré :

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

Lancez un terminal et 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 fréquemment posées

Comment trouver l'ordre (séquence) d'amorçage de la configuration de démarrage 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 matrice 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 périphériques de démarrage ?

Lors de la modification de la séquence d'amorçage, 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 matrice d'entrée du paramètre **Source**, est définie sur **0**, indiquant que le périphérique est désactivé.

Un message d'échec de connexion s'affiche lors de la connexion à l'espace de nom avec wbemtest. Comment résoudre ce problème ?

Lancez **wbemtest** avec des privilèges d'accès de niveau Administrateur pour éviter les messages de connexion. Ouvrez Internet Explorer dans la liste **Tous les programmes**, cliquez avec le bouton droit sur **Exécuter en tant qu'administrateur** pour lancer **wbemtest** et éviter les erreurs d'espace de nom.

Comment exécuter TechCenter Scripts sans problème ?

Voici les conditions préalables lors de l'exécution de scripts VBS fournis sur le lien Techcenter Dell Command | Monitor :

1. Configurez **winrm** sur le système en exécutant la commande `winrm quickconfig`.
2. Vérifiez que la prise en charge du jeton existe sur le système en vous référant à :
   - L'**écran F2** dans la configuration du BIOS.
   - Utilisez un outil tel que **wbemtest** pour vérifier que la valeur clé est définie 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 plus d'informations, voir le Guide de référence Dell Command | Monitor sur dell.com/dellclientcommandsuitemanuals.

Comment définir les attributs du BIOS ?

Les attributs du BIOS peuvent être modifiés en utilisant la méthode **DCIM_BIOSService.SetBIOSAttribute()**. 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**. Si le mot de passe du BIOS est défini sur le système, vous devez fournir le même mot de passe dans le cinquième argument. Les sixième et septième arguments peuvent également être vides ou NULL.

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

Oui, Dell Command | Monitor prend en charge à la fois la surveillance du stockage et de 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).

  REMARQUE : La surveillance de contrôleur intégré Intel n'est pas prise en charge sur les systèmes exécutant le système d'exploitation Linux.
- Contrôleurs RAID intégrés LSI ; et 9217, 9271, 9341, 9361 et leurs pilotes associés (physiques et logiques)

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

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

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

Oui, Dell Command | Monitor peut être associé aux principales consoles de gestion d'entreprise qui prennent en charge les standards 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.

9

Dépannage

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 :

- **Access Denied (Accès refusé)**
- **Win32:RPC server is unavailable (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'administrateur.
   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 qui exécute 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. Entrez le nom d'utilisateur sous la forme *<nom de la machine client>**<nom de 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, voir dell.com/dellclientcommandsuitemanuals.
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 **WMI tools** 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, voir la documentation Microsoft appropriée à l'adresse **http://msdn.microsoft.com**.

Échec d'installation sur les systèmes exécutant Windows

Si l'installation de l'outil Dell Command | Monitor sous Windows n'aboutit pas, vérifiez que :

- Vous détenez des privilèges d'administrateur sur le système cible.
- Le système cible est un système conçu par 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 Résumé système.

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

REMARQUE : Le système doit être mis à niveau vers .NET 4.0 ou version ultérieure.

La valeur d'énumération du paramètre BIOS est 1.

1. Vérifiez que les paquets 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 paquets ci-dessus sont installés, vérifiez que le module de pilotes est chargé.
   a. Vérifiez que le module de pilotes est chargé en exécutant la commande suivante `lsmod | grep dcdbas`.
   b. Si le module de pilote n'est pas disponible, récupérez les détails du pilote en exécutant la commande suivante `modinfo dcdbus`.
   c. Chargez le module de pilotes en exécutant la commande suivante `insmod <filename>`.

Échec de l’installation hapi en raison de la dépendance de la bibliothèque libsmbios

Si l’installation échoue en raison de problèmes de dépendance :

Forcez l’installation de tous les packages dépendants en exécutant `apt-get –f install`.

Ressources CIM non disponibles

Lors de l’énumération, si vous recevez un message d’erreur indiquant que les ressources CIM ne sont pas disponibles,

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 le paquet Snap installé sur le système est la version 2.23 ou ultérieure.

10

Contacter Dell

REMARQUE : Si vous ne disposez pas d'une connexion Internet, les informations de contact figurent sur la facture d'achat, le bordereau de colisage, la facture le catalogue des produits Dell.

Dell propose diverses options d'assistance et de maintenance en ligne et téléphonique. Ces options varient en fonction du pays et du produit et certains services peuvent ne pas être disponibles dans votre région. Pour contacter le service commercial, technique ou client de Dell :

1. Rendez-vous sur **Dell.com/support.**
2. Sélectionnez la catégorie d'assistance.
3. Rechercher 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 d'assistance approprié.

Autres documents utiles

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

- 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 *Dell Command | Monitor Guide de référence SNMP* fournit Simple Network Management Protocol (SNMP) Management Information Base (Base d'informations de gestion de Protocole de gestion de réseau simple (SNMP) (MIB) applicable à Dell Command | Monitor.

Accès aux documents à partir du site de support Dell EMC

Vous pouvez accéder aux documents requis en utilisant l'un des liens suivants :

- Pour les documents de gestion des systèmes Dell EMC Enterprise : **Dell.com/SoftwareSecurityManuals**
- Pour les documents Dell EMC OpenManage : **Dell.com/OpenManageManuals**
- Pour les documents Dell EMC Remote Enterprise Systems Management (Gestion des systèmes Enterprise à distance) : **Dell.com/esmmanuals**
- Pour les documents iDRAC et Dell EMC Lifecycle Controller : **Dell.com/idracmanuals**
- Pour les documents Dell EMC OpenManage Connections Enterprise Systems Management (Gestion des systèmes Enterprise - Connexions OpenManage) : **Dell.com/OMConnectionsEnterpriseSystemsManagement**
- Pour les documents Dell EMC Serviceability Tools (Outils de facilité de la gestion) : **Dell.com/ServiceabilityTools**
- Pour les documents Client Command Suite Systems Management : **Dell.com/DellClientCommandSuiteManuals**
- a. Accédez à **Dell.com/Support/Home**.
  b. Cliquez sur **Choisir parmi tous les produits**.
  c. Dans la section **Tous les produits**, cliquez sur **Logiciel et sécurité**, puis cliquez sur le lien requis parmi les suivants :
     – **Enterprise Systems Management (Gestion des systèmes Enterprise)**

- **Remote Enterprise Systems Management (Gestion des systèmes Enterprise à distance)**
- **Serviceability Tools (Outils de facilité de la gestion)**
- **Dell Client Command Suite**
- **Connections Client Systems Management (Gestion des systèmes Client - Connexions)**

d. Pour afficher un document, cliquez sur la version de produit requise.

- Avec les moteurs de recherche :
  - Saisissez le nom et la version du document dans la zone de recherche.