Dell Command | Monitor Version 9.0
Guide d'utilisation

Remarques, précautions et avertissements

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

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.

2014 - 09

Rev. A00

Table des matières

1

Introduction

Client Instrumentation désigne des applications logicielles qui activent la gestion à distance d'un système client. Le logiciel Dell Command | Monitor (Command | Monitor) permet à des programmes de gestion à distance à partir de programmes d'application pour accéder au système client de l'entreprise, de surveiller l'état ou de modifier l'état du système, tel que l'arrêt à distance du système. Command | Monitor utilise des paramètres système clés via des interfaces standard permettant aux administrateurs de gérer les stocks, de surveiller l'intégrité du système et de rassembler des informations des systèmes clients d'entreprise. 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.

Dell Command | MonitorPrésentation

Command | Monitor gère les systèmes clients à l'aide de la norme CIM (Common Information Model) et SNMP (Simple Network Management Protocol), qui sont des protocoles de gestion. Cela réduit le coût total de propriété, optimise la sécurité et fournit une approche intégrée pour gérer tous les périphériques, y compris les clients, les serveurs, le stockage, le réseau et les périphériques logiciels.

Grâce aux classes CIM, vous pouvez accéder à l'utilitaire Command | Monitor via WSMAN (Web Services for Management Standards).

Command | Monitor contient l'ensemble sous-jacent de pilotes qui collectent des informations des systèmes clients, à partir de sources diverses, y compris le BIOS, le CMOS, le SMBIOS (System Management BIOS), la SMI (System Management Interface - Interface de gestion du système), le système d'exploitation, les API (Application programming interface - Interface de programmation d'applications), les DLL (Dynamic-link library - Bibliothèques de liens dynamiques) et les paramètres de registre. Command | Monitor récupère ces informations au moyen de l'interface CIMOM (CIM Object Manager) de la pile WMI(Windows Management Instrumentation) ou de l'agent SNMP.

Command | Monitor permet aux administrateurs IT de collecter à distance des informations sur les actifs, de modifier les paramètres CMOS, de recevoir des notifications proactives en cas d'erreurs et des alertes en cas de violations de la sécurité. Ces alertes sont disponibles en tant qu'événements dans le journal des événements, l'indication CIM ou reçues sous forme d'interruptions SNMP après l'importation et la surveillance du fichier MIB (Management Information Base).

Command | Monitor sert à rassembler l'inventaire des actifs du système y compris les paramètres BIOS via l'implémentation CIM ou l'agent SNMP. Il peut être intégré à une console telle que Microsoft System Center Configuration Manager, en accédant directement aux informations CIM, ou via d'autres fournisseurs de consoles ayant implémenté l'intégration de Command | Monitor. En outre, vous pouvez

créer des scripts personnalisés pour cibler des zones d'intérêt clés. Vous pouvez utiliser ces scripts pour contrôler l'inventaire, les paramètres 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, voir le *Dell Command | Monitor Guide d'installation* disponible sur **dell.com/clientsystemsmanagement**.

Architecture Command | Monitor

Le fournisseur de données Command | Monitor collecte les données d'informations de système et les stocke au format exclusif XML. Le gestionnaire de données est un service qui charge ces fournisseurs selon la demande. La couche de fournisseur CIMCommand | Monitor extrait l'interface vers diverses implémentations CIMOM. L'entrée est une combinaison de données XML et XSL (Extensible Stylesheet Language) en format exclusif, alors que la sortie est une instance d'objet CIM basée sur les Profils de gestion. Le WSMAN,k qui sert de protocole de chaîne, demande les données au CIMOM et les transmet à la console.

L'architecture Command | Monitor comporte plusieurs couches qui sont intégrées à la pile WMI (Microsoft Windows Management Instrumentation) :

- Couche d'applications WMI : composée d'applications de gestion telles que les outils de gestion conformes aux normes, ainsi que des applications WMI telles que Microsoft SMS, LANDesk et les outils WMI. Les applications dans cette couche sont les consommateurs des données de gestion du système fournies par Command | Monitor. Ces applications demandent des informations de clients et envoient des alertes à l'aide de CIMOM (CIM Object Manager) WSMAN.
- Fournisseur CMI WMI : se situe en-dessous du CIMOM et contient deux fournisseurs CIM, qui sont enregistrés avec le CIMOM
  - Le fournisseur d'instance/de méthode implémente une interface permettant des opérations d'utilitaire telles que la création, la suppression, la modification et la requête.
  - Le fournisseur d'indications implémente une interface pour les indications WMI (ou événements).

    Lorsque le CIMOM reçoit une demande d'informations, il achemine la demande vers le fournisseur approprié. Tous les fournisseurs existent dans cette couche et fournissent des informations sur les périphériques de système. Les fournisseurs envoient des demandes d'application de gestion depuis le CIMOM vers le routeur de données.
- Gestionnaire de données : charge le fournisseur de données en fonction de la demande de la couche supérieure.
- Fournisseur de données : collecte les informations système telles que le matériel, les pilotes et les données du système d'exploitation , et les stocke au format XML exclusif.

L'architecture Command | Monitor comporte plusieurs couches supplémentaires qui sont intégrées à la pile SNMP :

- Agent SNMP : affiche les données reçues du gestionnaire de données sous forme de tables et d'interruptions SNMP.
- MIB : les fichiers MIB stockent des informations sur les tables SNMP, ses attributs et les interruptions disponibles.

Par exemple, une console de gestion dans la couche d'application WMI demande les informations de processeur disponibles sur un système client. La couche d'application WMI effectue la demande sur le réseau vers le CIMOM d'un système client. Le CIMOM transfère la demande vers le fournisseur et le gestionnaire de données CIMde Command | Monitor. Le gestionnaire de données charge le fournisseur

de données correspondant, qui récupère les informations et les stocke en format exclusif. Les informations sont alors renvoyées (par le même chemin en sens inverse) à la console de gestion.

Nouveautés de cette version

- Dell OpenManage Client Instrumentation (OMCI) est rebaptisé Dell Command | Monitor
- Prise en charge de la surveillance et des alertes du contrôleur LSI RAID (Redundant Array of Independent Disks (RAID)
- Prise en charge de la surveillance et des alertes de toutes les sondes de capteurs
- Les espaces de noms hérités **(root/dellomci)**ne sont pas pris en charge
- Prise en charge des nouvelles 10909 SNMP MIB
- Prise en charge des nouveaux jetons suivants :
  - Radio GPS
  - Rétro-éclairage du clavier en CA
  - Caméra arrière
  - Verrouillage <Fn>
  - Mode de verrouillage <Fn>
  - NIC(Carte d'interface réseau) intégrée non gérée
  - Unmanaged NIC
  - Rear USB Ports
  - Side USB Ports (Ports USB latéraux)
  - Trusted Execution
- Prise en charge de valeurs supplémentaires, **medium_high** et **medium_low** pour le jeton **fanspeed** (vitesse de ventilateur)

REMARQUE : Les espaces de noms hérités et MIB 10892 MIB SNMP ont été supprimés.

Pour en savoir plus sur les jetons, reportez-vous au *Guide de référence de Dell Command | Monitor* sur **dell.com/clientsystemsmanagement**.

Fonctions

Les principales fonctionnalités de Command | Monitor sont les suivantes :

- Prise en charge du schéma CIM 2.17
- Configuration BIOS
- Sécurité WMI
- Rapport d'événements
- Arrêt à distance
- Accès aux informations système à l'aide du protocole WMI-CIM, de WSMAN et de SNMP
- Compilation des informations détaillées d'actifs
- 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 Intel et LSI.

- Surveillance et interruptions SNMP

Prise en charge du schéma CIM 2.17

Command | Monitor se conforme au schéma CIM 2.17 et inclut deux fournisseurs WMI :

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

Configuration BIOS

Command | Monitor offre la possibilité de configurer un BIOS système, notamment la gestion de sa séquence d'amorçage.

Sécurité WMI

WMI authentifie l'utilisateur avant d'accorder l'accès aux données et méthodes CIM. Les privilèges d'accès sont contrôlés par la sécurité DCOM (Distributed Component Object Model) et par CIMOM. L'accès, total ou limité, peut être accordé aux utilisateurs par espace de nom. Il n'existe aucune implémentation de classe ou sécurité au niveau de la propriété. Par défaut, les utilisateurs membres du groupe d'administrateurs possèdent un accès total local et distant à WMI.

La sécurité WMI peut être configurée à l'aide de la Commande WMI disponible dans la console Computer Management sous la section Services et applications. Effectuez un clic droit sur **Contrôle WMI**, puis cliquez sur **Propriétés**. Vous pouvez configurer la sécurité spécifique aux espaces de nom depuis l'onglet **Sécurité**. **Contrôle WMI** peut aussi être exécutée depuis le menu **Démarrer** ou de la **CLI**, en exécutant `wmimgmt.msc`.

Rapport d'événements

Command | Monitor détecte les événements sur les systèmes Dell et alerte l'utilisateur local et l'administrateur réseau au sujet d'éventuelles pannes, modifications de configuration et intrusions dans le châssis. Ces événements sont affichés par une application de gestion des systèmes, telle que Open Manage Essentials (OME).

Arrêt à distance

Command | Monitor prend en charge l’arrêt et le redémarrage à distance de systèmes.

Accès aux informations

Command | Monitor fournit un accès aux informations système telles que la révision BIOS et le modèle de système au moyen de WMI à l'aide de CIM. Le protocole WSMAN peut aussi être utilisé pour accéder à ces informations au moyen de WMI.

Informations d'inventaire détaillées

Command | Monitor fournit l'accès aux informations d'inventaire détaillées telles que les processeurs, périphériques PCI et batteries.

Configuration des paramètres de réveil à distance

Command | Monitor prend en charge la configuration des paramètres de réveil à distance. Réveil à distance est une fonction du système client et de la carte NIC (Network Interface Card).

Modification à distance des paramètres système

Command | Monitor permet aux administrateurs de récupérer et définir des paramètres du BIOS de clients commerciaux tels que la configuration de ports USB, l'ordre d'amorçage et les paramètres NIC.

État et intégrité du système

Command | Monitor contrôle l'intégrité du système comme par exemple l'état du ventilateur et en rapporte l'état via les entrées de journal d'événement NT et les événements CIM.

Surveillance et alertes RAID pour les contrôleurs Intel et LSI.

Surveillance et alertes des lecteurs logiques et physiques des contrôleurs RAID Intel et LSI.

Surveillance et interruptions SNMP

Command | Monitor confirme à SNMP v1 et prend en charge la surveillance des attributs système et des interruptions.

2

Normes et protocoles

Command | Monitor utilise Microsoft Windows Management Instrumentation (WMI) et active les protocoles Web Services-Management (WSMAN). Command | Monitor utilise Simple Network Management Protocol (SNMP) pour décrire plusieurs variables du système.

Présentation des technologies CIM, SNMP, WMI et WSMAN

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.

CIM

Créé par le consortium DMTF dans le cadre de l'initiative de gestion de réseau basée sur le Web (WBEM), le modèle CIM offre une vue unifiée d'objets physiques et logiques dans l'environnement géré.

Les informations suivantes concernant le modèle CIM sont importantes :

- CIM est un modèle de données orienté objet, servant à décrire les informations de gestion. CIMdécrit la façon dont les données sont organisées et non nécessairement le modèle de transport utilisé pour transporter les données. La méthode de transport la plus courante est WMI.
- Les applications de gestion compatibles CIM rassemblent les informations à partir de divers objets et périphériques CIM, comprenant des systèmes client et serveur, des périphériques d'infrastructure réseau et des applications.
- La spécification CIM détaille des techniques d'adressage permettant une compatibilité améliorée avec d'autres protocoles de gestion.
- Le modèle de données CIM résume et décrit tous les éléments d'un environnement réseau. Le schéma CIM fournit les descriptions de modèle de données et organise le réseau dans une série d'objets gérés, tous liés entre eux et classés globalement.
- Le schéma CIM est défini par le fichier MOF (Managed Object Format), qui fournit un modèle standardisé pour la description d'informations de gestion entre les clients d'un système de gestion. Le fichier MOF n'est lié à aucune implémentation particulière et facilite l'échange d'informations de gestion entre différents systèmes de gestion et clients .

SNMP

Simple Network Management Protocol (SNMP) est une solution largement acceptée pour la gestion des périphériques sur les réseaux IP. SNMP est développé et conservé par IETF (Engineering Task Force). Command | Monitor accède aux informations et surveille les systèmes clients par l'intermédiaire de SNMP. Parmi les périphériques qui prennent typiquement en charge SNMP on compte les routeurs, les commutateurs, les serveurs, les stations de travail, la plupart des composants matériels et plus encore. Il s'agit d'un ensemble de normes de gestion de réseau, notamment un protocole de couche

d'applications, un schéma de base de données et un ensemble objets de données. SNMP expose les données de gestion sous forme de variables sur les systèmes gérés, qui décrivent la configuration du système. Ces variables peuvent alors être interrogées via la gestion des applications.

SNMP ne définit pas quelles informations (variables) sont offertes par un système géré. SNMP utilise plutôt une conception extensible, où la liste des informations disponibles est définie par les bases d'informations de gestion (MIB). Les MIB décrivent la structure des données de gestion d'un périphérique et de ses sous-systèmes. Les MIB utilisent un espace de nom hiérarchique contenant des object identificateurs d'objet (OID). Chaque OID identifie une variable lisible via SNMP.

WMI

WMI est l'implémentation Microsoft de l'effort WBEM (Web-based Enterprise Management). Il est implémenté sur les plateformes Microsoft Windows. WMI prend en charge CIM et les extensions CIM spécifiques à Microsoft.

WMI inclut :

- Un ensemble puissant de services natifs tels que la récupération d'informations et la notification d'événements à base de demande.
- Des capacités de script via WSH (Windows Scripting Host).
- Le CIMOM, qui est le point d'interface et de manipulation pour les objets et informations CIM.
- La logithèque, où CIMOM stocke les données de gestion.

Dans l'architecture Command | Monitor, CIMOM et le stockage sont représentés par le Microsoft WMI Object Manager. Le CIMOM est l'interface et le point de manipulation des objets et informations CIM. Il facilite la collecte d'informations et la manipulation de propriétés d'objets. Microsoft a implémenté ce composant en tant que service de gestion Windows (winmgmt). Le CIMOM est un logiciel de couche moyenne qui sert de médiateur entre les applications de gestion à haut niveau et les infrastructures de niveau inférieur, tels qu'OMCI et d'autres fournisseurs. Le CIMON garantit que les données fournies par les fournisseurs sont présentées aux applications de gestion de façon uniforme et indépendante du fournisseur. Pour ce faire, le CIMOM se sert de l'interface API (Application Programming Interface) du COM (Component Object Model).

Le référentiel est un fichier binaire dans lequel le CIMOM stocke des données de gestion. Celles-ci comprennent des informations du/des fichier(s) MOF (Managed Object Format) compilé(s), y compris les définitions de classe CIM, propriétés, qualificateurs et relations hiérarchiques CIM. Les données d'instance sont aussi stockées ici au fur et à mesure qu'elles sont disponibles.

WMI fournit une interface de scriptage. À l'aide de VBScript ou JScript, vous pouvez écrire des scripts, vous connecter aux services WMI localement ou à distance, récupérer des informations ou exécuter des méthodes. Vous pouvez créer un script pour la plupart des tâches Command | Monitor car Command | Contrôle est implémenté au moyen de WMI.

Pour plus d'informations sur VBScript et des exemples de scripts, voir le *Guide de référence de Dell Command | Monitor* à l'adresse **dell.com/clientsystemsmanagement**.

Pour plus d'informations concernant WMI voir **technet.microsoft.com**.

REMARQUE : Pour vous connecter à distance aux services WMI, vous devez posséder des droits d'administrateur sur les systèmes locaux et distants.

WSMAN

Le Protocole WSMAN (WS-Management) est une norme ouverte DMTF qui définit un protocole SOAP (Simple Object Access Protocol) pour la gestion de serveurs, périphériques, applications et services Web. Il utilise les données de CIMOM pour faciliter la gestion.

WSMAN est un protocole qui fournit une couche d'abstraction permettant d'accéder aux informations CIM, la raison étant que la console peut utiliser WSMAN pour communiquer avec les systèmes intrabande ou hors bande afin de recueillir un inventaire d'actifs et de définir des informations ou d'exécuter des méthodes. Dans les systèmes intrabandes, la couche WSMAN résume aussi le système d'exploitation sous-jacent. Cependant, Command | Monitor n'exige pas WSMAN et n'active pas directement WSMAN, car il ne s'agit que d'un protocole.

Pour en savoir plus sur la gestion de WSMAN à partir de DMTF, voir : **dmtf.org/standards/wsman/**

Pour plus d'informations sur l'activation de la gestion WSMAN de WMI sur un système exécutant le système d'exploitation Windows, voir **msdn.microsoft.com/en-us/library/aa384426 %28v = VS.85% 29.aspx**.

Pour plus d'informations sur les profils DMTF utilisés dans l'utilitaire Command | Monitor, consultez le *Guide de référence de Dell Command | Monitor* à l'adresse **dell.com/clientsystemsmanagement**.

PowerShell

Windows PowerShell est une infrastructure Microsoft de gestion de la configuration et de l'automatisation des tâches. PowerShell se compose d'un interpréteur de ligne de commande et du langage de script associé qui reposent sur .NET Framework. PowerShell offre un accès complet à COM et WMI, ce qui permet aux administrateurs d'effectuer des tâches d'administration telles que la configuration et la surveillance sur les systèmes locaux et à distance fonctionnant sous le système d'exploitation Windows utilisant les services de Command | Monitor.

Les administrateurs peuvent créer des scripts PowerShell (dont le suffixe est **.ps1**) qui se connectent à l'espace de noms DCIM et permettent la surveillance des actions personnalisées sur le système.

3

Configuration système requise

Ce chapitre fournit des informations sur la configuration matérielle et logicielle requise de Command | Monitor.

Configuration matérielle requise

Exigence	Détails
Système	Système Enterprise Client doté de SMBIOS 2.3 ou version ultérieure.

Configuration logicielle requise

Exigence	Détails
Système d'exploitation pris en charge	• Microsoft Windows 8.1 • Microsoft Windows 8 • Microsoft Windows 7 • Microsoft Windows Vista
Infrastructure prise en charge	• Microsoft .NET 4.0

4

Scénarios d'utilisation

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

Vous pouvez utiliser Command | Monitor pour :

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

Scénario 1 : Gestion de l'inventaire

Une société qui utilise plusieurs systèmes Dell n'a pas pu conserver des informations d'inventaire exactes en raison de changements de personnel commercial et IT. Le Directeur informatique demande un plan pour identifier les systèmes qui peuvent être mis à niveau aux dernières versions de Microsoft Windows. Cela exige une évaluation des systèmes déployés pour déterminer la taille, l'étendue et l'impact financier d'un tel projet. La collecte d'informations demande un effort considérable. Le déploiement de personnel IT vers chaque système client coûte cher du point de vue heures de travail et interruptions pour les utilisateurs finals.

À l'aide de l'utilitaire Command | Monitor sur chaque système Dell, le responsable des services informatiques peut rapidement collecter des informations à distance. En utilisant des outils tels que Microsoft System Center Configuration Manager (SCCM), le responsable des services informatiques 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 actuelle du système d'exploitation. Une fois collectées, les informations peuvent être analysées pour déterminer les systèmes qui peuvent être mis à niveau à l'aide des versions Windows les plus récentes.

Vous pouvez également obtenir un inventaire des actifs à l'aide d'un script ou d'une ligne de commande WMI (Windows Management Instrumentation).

Intégration SCCM

Vous pouvez intégrer SCCM à Command | Monitor en :

- Utilisant le fichier MOF au sein du progiciel d'installation Command | Monitor, qui contient toutes les classes de Command | Monitor et en effectuant une importation vers ConfigMgr

  Le fichier MOF se trouve à l'emplacement suivant :

  C:\Program Files\Dell\Command_Monitor\ssa\omacim\OMCI_SMS_DEF.mof
- 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 clients et de gérer chaque système tout au long de son cycle de vie. Dans le cadre de cet effort, la société achète un nouvel ensemble d'outils et prévoit d'automatiser le déploiement d'un nouveau système d'exploitation client à l'aide du PXE (Preboot Execution Environment).

Le défi consiste à modifier le paramètre de séquence d'amorçage dans le BIOS de chaque ordinateur client sans avoir à se déplacer. Une fois l'utilitaire Command | Monitor installé sur chaque système client, le service informatique de la société dispose de plusieurs options pour modifier à distance l'ordre d'amorçage. OpenManage Essentials (OME) est une console de gestion qui peut être utilisée pour contrôler à distance les paramètres du BIOS sur tous les systèmes Enterprise du client. Une autre option consiste à écrire un script VB/PowerShell/WMIC) qui modifie les paramètres de séquence d'amorçage. Le script peut être transmis à distance via le réseau et exécuté sur chaque système client.

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

Les configurations standardisées peuvent faire représenter de grandes économies pour les sociétés, quelle que soit leur taille. De nombreux organismes déploient des systèmes clients standardisés, mais peu d'entre eux gèrent la configuration système tout au long du cycle de vie de l'ordinateur. Avec Command | Monitor installé sur chaque système client, le service informatique peut verrouiller les ports Hérités pour prévenir l'utilisation de périphériques non autorisés ou activer WOL (Wake On LAN) pour que le système puisse être mis hors mode Veille en dehors des heures de pointe pour réaliser des tâches de gestion de systèmes.

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 celui-ci semble s'être résolu. Entretemps, 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. Command | Monitor affiche aussi une erreur SMART pour 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 de sauvegarder les fichiers de données essentiels immédiatement. On fait intervenir un technicien de service qui arrive avec un disque 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 événements système par l'intermédiaire de Windows Event Viewer ou d'indication CIM

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

- Extraction du journal par l'intermédiaire de la classe **DCIM_LogEntry**.
- Surveillance de l'indication CIM par l'intermédiaire de la classe **DCIM_AlertIndication**.

- Surveillance des événements par l'intermédiaire de Simple Network Management Protocol (SNMP).

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

Scénario 4 : Profils

Les administrateurs IT se voient obligés de gérer le système client Dell dans des environnements d'entreprise multi-fournisseurs et répartis. Ils doivent relever de nombreux défis car ils doivent maîtriser divers jeux d'outils et d'applications tout en gérant plusieurs systèmes clients de bureau ou mobiles dans divers réseaux. Afin de réduire le coût imposé par ces exigences et de représenter les données de gestion fournies, les profils standard de l'industrie DMTF(Distributed Management Task Force) et DCIM-OEM (Data Center Infrastructure Management) sont implémentés dans Command | Monitor. Certains profils DMTF sont expliqués dans ce guide.

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

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 la valeur de l'attribut BIOS peut être modifiée 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 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 Command | Monitor en vous rendant sur :

- root\dcim\sysman (standard)

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/clientsystemsmanagement**.

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 capacité du disque, l'augmentation/réduction de mémoire, l'augmentation/réduction du nombre de processeurs, en vous servant des fichiers dcsbdy32.ini ou dcsbdy64.ini. Le fichier dcsbdy32/64.ini se trouve à l'emplacement suivant :

<Command | Monitor installed location>\omsa\ini

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

Rapport d'état de RAID

Command | Monitor active les informations de configuration de RAID et surveille la fonctionnalité RAID pour les systèmes clients dotés de prise en charge de matériel et de pilotes. Utilisez les classes RAID pour obtenir des détails concernant les niveaux de RAID, des informations sur les pilotes, la configuration du contrôleur et la condition du contrôleur. Une fois la configuration du RAID activée, vous pouvez recevoir des alertes concernant la dégradation ou les pannes des lecteurs et des contrôleurs.

REMARQUE : Le rapport d'état de RAID est pris en charge uniquement par les contrôleurs RAID fonctionnant avec des pilotes compatibles avec CSMI (Common Storage Management Interface) version 0.81. OMCI 8.1 et les versions ultérieures ne prennent en charge la surveillance que sur le contrôleur sur puce RAID Intel. À partir d'OMCI 8.2, les alertes concernant le contrôleur sur puce RAID Intel sont prises en charge. Command | Monitor 9.0 et les versions ultérieures prennent aussi en charge la surveillance des contrôleurs LSI et la fonction d'alerte .

Surveillance des systèmes clients

Command | Monitor prend en charge le protocole SNMP (Simple Network Management Protocol) pour surveiller et gérer les systèmes clients tels que les portables, les ordinateurs de bureau et les stations de travail. Le fichier MIB (Management Information Base) est partagé entre Command | Monitor et l'administrateur du serveur (Server Administrator).

À partir de la version 9.0, Command | Monitor a été modifié pour utiliser un OID spécifique au client OID (10909) pour que les consoles identifient les systèmes client.

Pour en savoir plus sur SNMP, reportez-vous au *Dell Command | MonitorGuide de reférence SNMP* sur **dell.com/clientsystemsmanagement**.

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) de secteur à 512 octets. Les disques durs basculant vers les secteurs 4Ko conservent la compatibilité arrière, alors que les disques durs AF actuels, aussi nommés disques durs 512e, correspondent au SATA 512 octets et fonctionnent à 4Ko. 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 secteur qui traitent les disques 512e. Command | Monitor vous permet de savoir si le disque dur d'un système est un disque AF 4Ko, ce qui aide à éviter les problèmes susmentionnés.

Configurations d'amorçage

Un système d'ordinateur client peut avoir deux configurations d'amorçage :

- Hérité (BIOS)
- UEFI

Dans Dell Command | Monitor, la configuration d'amorçage (Héritée ou UEFI) est modélisée à l'aide des 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 Héritée 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 l'instance de **DCIM_BootConfigSetting** aux instances de **DCIM_BootSourceSetting** représentant un des types de liste d'amorçage (Hérité ou UEFI), auquel les périphériques de démarrage appartiennent. La propriété **GroupComponent** de **DCIM_OrderedComponent** réfère à l'instance **DCIM_BootConfigSetting** et la propriété **PartComponent** réfère à l'instance **DCIM_BootSourceSetting**.

Modification de la séquence d'amorçage à l'aide de la méthode ChangeBootOrder

Pour modifier la séquence de démarrage, 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`
   - PowerShell Command : `gwmi -namespace root\dcim\sysman -class dcim_BootConfigSetting -Property ElementName`
2. Rechercher le type de commande de démarrage (hérité ou UEFI) à l'aide de :
   - Commande WMIC : `wmic /namespace:\\root\dcim\sysman path dcim_BootConfigSetting get ElementName/format:list`
   - PowerShell Command : `gwmi -namespace root\dcim\sysman -class dcim_elementSettingData -Filter "IsCurrent=1" -Property SettingData`
3. Modifiez la séquence d'amorçage à l'aide de :
   - La commande WMIC : `wmic /namespace:\\root\dcim\sysman path dcim_bootconfigsetting call ChangeBootOrder /?:full`
   - PowerShell Command : `gwmi -namespace root\dcim\sysman -class dcim_BootConfigSetting -Property ElementName`

   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 provenant de la propriété DCIM_OrderedComponent.PartComponent. La nouvelle séquence d'amorçage est déterminée par l'ordre des périphériques d'amorçage dans le tableau **source** .

Définition des attributs BIOS

Dans Dell Command | Monitor, les méthodes suivantes sont ajoutées pour la modification des paramètres système et de l'état des systèmes locaux ou à distance :

- **SetBIOSAttributes** : pour la modification du paramètre BIOS
- **ChangeBootOrder** : pour la modification de la configuration de démarrage
- **RequestStateChange** : pour arrêter et redémarrer le système
- **ManageTime** : renvoie l'heure du système

Vous pouvez invoquer ces méthodes à l'aide de winrm, d'un script VB, des commandes Powershell, de wmic, de wbemtest.exe et de WMI wbemtest.

Vous pouvez définir les attributs BIOS à l'aide de la méthode SetBIOSAttributes. La procédure est expliquée ci-dessous en activant le 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 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 :

   ```
   (gwmi -Class DCIM_BIOSService -Namespace root\dcim
   \sysman).SetBIOSAttributes($null,$null,"AdminPwd","entrez un nouveau mot de
   passe")
   ```

2. Pour activer la sécurité du module de plateforme sécurisée, utilisez la commande suivante, puis redémarrez le système :

   ```
   (gwmi -Class DCIM_BIOSService -Namespace root\dcim
   \sysman).SetBIOSAttributes($null,$null,"Trusted Platform Module","1","
   saisissez le mot de passe")
   ```

3. Pour activer le module de plateforme sécurisée (TPM), utilisez la commande suivante et redémarrez le système :

   ```
   (gwmi -Class DCIM_BIOSService -Namespace root\dcim
   \sysman).SetBIOSAttributes($null,$null,"Trusted Platform Module
   Activation","2"," saisissez le mot de passe")
   ```

4. Redémarrez le système.

   REMARQUE : Utilisez PowerShell avec les privilèges d'administrateur.

6

Questions fréquemment posées

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

Lorsqu'une instance (Héritée ou UEFI) **DCIM_BootConfigSetting** comporte plusieurs instances **DCIM_BootSourceSetting** (périphériques d'amorçage) et y est associée par le biais d'instances de l'association **DCIM_OrderedComponent**, la valeur de la propriété **DCIM_OrderedComponent.AssignedSequence** est utilisée pour déterminer la séquence selon laquelle les instances **DCIM_BootSourceSetting** (périphériques d'amorçage) sont utilisées lors du processus de démarrage. Un **DCIM_BootSourceSetting** dont la propriété **CIM_OrderedComponent.AssignedSequence** associée est égale à **0** est ignoré et n'est pas considéré comme faisant partie de la séquence de démarrage.

Comment modifier la séquence d'amorçage ?

La séquence d'amorçage peut être modifiée à l'aide de 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 a un paramètre d'entrée : **Source**. Le paramètre **Source** est une matrice ordonnée de propriété **PartComponent** de la classe **DCIM_OrderedComponent** qui représente l'association entre les instances **DCIM_BootSourceSetting** (périphériques d'amorçage) et l'instance **DCIM_BootConfigSetting** (type de liste d'amorçage Hérité ou UEFI).

Comment désactiver les périphériques d'amorçage ?

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 puis-je contourner le problème ?

Lancez **wbemtest** avec un niveau de privilège d'administrateur pour contourner les messages de connexion. Localisez l'Internet Explorer à partir de la liste **Tous les programmes**, cliquez droit sur **Exécuter en tant qu'administrateur** pour démarrer **wbemtest** et éviter les erreurs d'espace de nom.

Comment exécuter TechCenter Scripts sans problèmes?

Ci-après se trouvent les conditions requises lors de l'exécution des scripts VBS fournis dans le lien Techcenter Command | Monitor :

1. Veuillez configurer **winrm** sur le système à l'aide de 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**.

Comment définir les attributs BIOS ?

Modifiez les attributs BIOS à l'aide de la méthode **DCIM_BootService.SetBIOSAttributes()**. La méthode **SetBIOSAttributes()** définit la valeur de l'instance définie dans la classe **DCIM_BIOSEnumeration**. La méthode possède sept paramètres d'entrée. Les deux premiers paramètres peuvent être vides ou nuls. Le troisième paramètre **AttributeName** doit faire passer le mappage d'entrée à la valeur de l'instance du nom d'attribut de la classe **DCIM_BIOSEnumeration**. Le quatrième paramètre ou **AttributeValue** peut être n'importe laquelle des valeurs possibles du nom d'attribut définies dans la classe **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 nuls.

7

Dépannage

Impossible de se connecter à distance à Windows Management Instrumentation (Infrastructure de gestion Windows)

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:RPC server is unavailable (Win32 : le serveur RPC n'est pas disponible)**

1. Pour vérifier que le système client est connecté au réseau, à l'invite de commande du serveur, entrez :

   `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 : Sauvegardez vos fichiers de données de système avant de modifier le registre. Le fait de modifier incorrectement le registre peut rendre votre système d'exploitation inutilisable.
3. Modifiez le registre sur le système client. Cliquez sur **Démarrer** → **Exécuter**, entrez **regedit**, puis cliquez sur **OK**. Dans la fenêtre **Éditeur de registre**, naviguez vers My Computer \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
4. Définissez la valeur **forceguest** sur **0** (la valeur par défaut est **1**). À moins que vous ne modifiiez cette valeur, l'utilisateur se connectant à distance au système détient des privilèges d'invité, même si les références fournies garantissent 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 l'utilitaire IT Assistant ConfigServices (**configservices.exe** disponible dans le répertoire **/bin** sous le répertoire d'installation IT Assistant). Configurez IT Assistant pour qu'il s'exécute sous un compte administrateur local, qui est également maintenant un administrateur sur le client à distance. Vérifiez aussi que DCOM et CIM sont activés.
   c. Si vous utilisez IT Assistant, utilisez le compte administrateur pour configurer la découverte de sous-réseau pour le système client. Entrez le nom d'utilisateur sous la forme *<nom d'ordinateur client>\<nom de compte>*. Si le système a déjà été découvert, supprimez le système de la liste de systèmes découverts, configurez sa découverte de sous-réseau, puis redécouvrez-le.

REMARQUE : Dell vous conseille d'utiliser Dell OpenManage Essentials à la place d'IT Assistant. Pour plus d'informations sur Dell OpenManage Essentials, reportez-vous à la rubrique **dell.com/clientsystemsmanagement**.

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 à l'aide de 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 du système en conséquence 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. Se connecter à l'infrastructure WMI (**root\DCIM/SYSMAN**) sur le système local à partir d'un système distant à l'aide de WMI wbemtest. Par exemple, \\[Adresse IP du système distant cible] \racine\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 de l'installation

If you are unable to complete Dell Command | Monitor installation, ensure that:

- You have Administrator privilages on the target system.
- The target system is a Dell manufactured system with SMBIOS version 2.3 or later.

REMARQUE : To check the SMBIOS version on the system, go to **Start** → **Run** and run the **msinfo32.exe** file and check for the SMBIOS version in System Summary page.

REMARQUE : The system must be running supported Microsoft Windows operating system.

REMARQUE : The sytsem has to be upgraded to .NET 4.0 or later versions.

8

Contacter Dell

REMARQUE : Si vous ne disposez pas d'une connexion Internet, les informations de contact figurent sur la facture d'achat, le borderau 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 à l'adresse **dell.com/clientsystemsmanagement**. Cliquez sur Command Monitor (Contrôle de commande) (anciennement OpenManage Client Instrumentation), puis cliquez sur le lien de produit approprié dans la section de **Support général** .

- Le *Dell Command | Monitor Guide de référence* fournit des informations détaillées sur l'ensemble des classes d'instrumentation Client, leurs propriétés et leurs descriptions.
- Le *Dell Command | MonitorGuide d'installation* fournit des informations sur l'installation de Client Instrumentation client.
- 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

Vous pouvez accéder aux documents requis de l'une des façons suivantes :

- À l'aide des liens suivants :
  - Pour tous les documents Enterprise Systems Management : **dell.com/softwaresecuritymanuals**
  - Pour les documents Enterprise System Management : **dell.com/openmanagemanuals**
  - Pour les documents Remote Enterprise System Management : **dell.com/esmmanuals**
  - Pour les documents de gestion des systèmes OpenManage Connections Enterprise : **dell.com/OMConnectionsEnterpriseSystemsManagement**
  - Pour les documents Serviceability Tools : **dell.com/serviceabilitytools**
  - Pour les documents Client System Management : **dell.com/clientsystemsmanagement**

- Pour les documents de gestion des systèmes OpenManage Connections Client : **dell.com/connectionsclientsystemsmanagement**

- Sur le site de support Dell :

  a. Rendez-vous sur **dell.com/support/manuals**.

  b. Dans la section **General support** (Support général), cliquez sur **Software & SecurityLogiciel et sécurité** (Logiciels et sécurité).

  c. Dans la zone de groupe **Software & Security** (Logiciels et sécurité), cliquez sur le lien approprié parmi les liens suivants :

     - **Enterprise Systems Management**
     - **Remote Enterprise Systems Management**
     - **Serviceability Tools**
     - **Client Systems Management**
     - **Connexions Client Systems Management**

  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 .