BITDEFENDER
BUSINESS SOLUTIONS

Utilisation des scripts WMI pour améliorer la visibilité du réseau et faciliter une administration opérationnelle

Présentation de la solution

Bitdefender

TABLE DES MATIÈRES

Bitdefender

1. INTRODUCTION

On attend de nombreux services informatiques qu'ils fonctionnent efficacement, avec souvent peu de ressources, et mettent en œuvre en un minimum de temps des procédures et des moyens proactifs pour limiter l'exposition aux menaces. Les petites et moyennes entreprises (PME) ont des exigences encore plus fortes liées à des budgets restreints et il est fréquent que les tâches informatiques soient accomplies par un employé occupant une double fonction, et non spécialisé.

Face à de telles exigences financières et informatiques, le personnel informatique débordé a du mal à installer et à maintenir des solutions de sécurité, et à gérer le réseau. La solution à ce problème consiste à simplifier et à automatiser les tâches manuelles répétitives, afin d'aider à améliorer la sécurité globale du réseau et de faciliter le reporting de conformité.

Lorsqu'une entreprise se développe, l'arrivée de nouveaux employés, l'utilisation de nouveaux systèmes et d'applications augmente la complexité de son réseau. Chaque nouveau poste de travail, ordinateur portable ou serveur, doit être géré par le service informatique, ce qui diminue sa capacité à assurer son rôle de surveillance et complique ses tentatives de visualiser ce qui est effectivement en train de se produire sur le réseau. Pour être proactifs et travailler plus efficacement, les services informatiques doivent s'assurer de disposer d'outils simples et performants capables de les aider à accomplir automatiquement des tâches répétitives et manuelles, tout en leur apportant une meilleure visibilité des dispositifs et des applications nécessaires aux activités de l'entreprise. Les outils d'automatisation peuvent rapidement déceler les brèches de la sécurité comme l'utilisation non autorisée de faux antimalwares ou de matériel inconnu utilisant des services qui vont davantage exposer l'organisation à des risques, y compris à la perte de données, à la contamination de malwares et à l'invasion de virus.

2. PRÉSENTATION DE LA TECHNOLOGIE D'INFRASTRUCTURE DE GESTION WINDOWS (WMI)

L'infrastructure de gestion Windows (WMI) est une mise en œuvre de l'initiative WBEM (Web-Based Enterprise Management), une initiative pour définir des normes d'accès et de partage d'informations de gestion dans un réseau d'entreprise. WMI respecte les normes WBEM et fournit un support intégré pour le modèle CIM (Common Information Model), le modèle de données décrivant les objets existant dans un environnement de gestion.

WMI permet à l'administrateur réseau de gérer à distance les serveurs et les postes de travail Windows déployés sur leur réseau à l'aide de scripts conformes aux normes de l'industrie. Les scripts WMI peuvent être exécutés uniquement sur les stations de travail sur lesquelles les services WMI sont installés. WMi est pré-installé avec Windows 7, Windows Vista, Windows Server 2008, Windows Server 2003, Windows XP, Windows Me, et Windows 2000.

Pour simplifier la tâche des ressources informatiques des PME, les solutions Bitdefender pour Entreprises comprennent différentes fonctionnalités pour une gestion automatisée du réseau afin d'apporter à ses clients l'offre la plus avantageuse. Citons parmi ces fonctionnalités la prise en charge de scripts WMI.

La mise en place et le déploiement d'une solution d'automatisation personnalisée constitue généralement un défi de taille. Afin d'éviter le travail de recherche et de développement de tâches, Bitdefender propose 30 modèles prédéfinis utilisant la norme WMI.

Bitdefender Management Server est la seule solution antimalware pour entreprises à intégrer directement les scripts WMI dans son composant de gestion, pour un coût total de possession inférieur à celui d'autres solutions grâce à son interface complète et facile à utiliser. Il peut être configuré pour exécuter des scripts WMI sur des groupes de stations de travail du réseau et offre des outils de planification afin de réduire la charge administrative et de centraliser les résultats pour le reporting. Les administrateurs IT peuvent ainsi effectuer un audit du réseau (recueillir des informations sur le matériel ainsi que sur les systèmes de stations de travail et de serveurs Windows) et des tâches administratives à distance.

Pour plus d'informations sur WMI, veuillez consulter la section Windows Management Instrumentation *du site de Microsoft Developer Network (MSDN).*

3. CINQ RAISONS D'INTÉGRER UNE SÉCURITÉ ANTIMALWARE AVEC AUDIT RÉSEAU ET ADMINISTRATION DES SYTÈMES

Certaines entreprises n'ont pas les moyens d'investir dans un logiciel spécialisé d'administration des ressources, mais elles ont pour la plupart besoin d'être informées des logiciels installés sur leur réseau pour être en conformité avec les obligations financières, gouvernementales ou industrielles.

Pour les aider à résoudre ce problème la Console d'Administration Centralisée de Bitdefender peut être configurée pour recueillir quotidiennement des informations sur les systèmes déployés sur le réseau, ce qui fournit aux responsables informatiques un inventaire à jour par le biais de rapports et leur apporte une visibilité des ressources réseau pour répondre à tout audit interne ou externe.

L'intégration de l'audit réseau et de l'administration du système permet aux entreprises de :

1. Simplifier l'administration du réseau et réduire la charge liée au reporting manuel
2. Automatiser la collecte des données de l'audit du réseau pour les rapports d'inventaire et de modifications
3. Assurer la conformité avec les licences logicielles et identifier les applications non autorisées
4. Réduire les coûts liés à l'administration d'un système d'inventaire séparé et d'agents sur les postes de travail
5. Identifier le matériel/les logiciels ne répondant pas à la configuration minimale requise par la politique de l'organisation

1. SIMPLIFIER L'ADMINISTRATION DU RÉSEAU ET REDUIRE LA CHARGE LIÉE AU REPORTING MANUEL

Bitdefender Management Server permet au personnel du service informatique d'être plus efficace en exécutant des tâches réseau à distance via une interface simple, avec assistant. Il permet une configuration pas à pas de tous les paramètres de script nécessaires, avec exécution immédiate ou programmée sur les ordinateurs ou les groupes d'ordinateurs du réseau sélectionnés.

Les tâches réseau peuvent gérer à distance les applications installées et les processus ou services en cours, le processus Windows Update, ou délimiter l'accès aux périphériques amovibles USB. Ces modifications de la configuration de l'administration peuvent s'appliquer globalement aux systèmes Windows sélectionnés sur réseau, ce qui permet aux équipes informatiques de consacrer plus de temps à des fonctions plus importantes et moins fastidieuses.

2. AUTOMATISER LA COLLECTE DES DONNÉES DE L'AUDIT DU RÉSEAU POUR LES RAPPORTS D'INVENTAIRE ET DE MODIFICATIONS

Les contraintes réglementaires et liées au reporting financier interne créent le besoin, dans de nombreuses organisations, du reporting et de l'audit réseau automatisés. Certaines obligations de reporting sont imposées par l'industrie des cartes de paiement (PCI), les lois HIPAA (Health Insurance portability and Accountability Act) et Sarbanes-Oxley (SOX) ou par d'autres autorités financières.

Les fonctionnalités d'audit réseau présentes dans la console d'Administration Centralisée de Bitdefender exploitent les scripts WMI en permettant aux administrateurs informatiques de créer des aperçus de configuration logicielle et matérielle. Les informations logicielles et matérielles recueillies sont disponibles à la demande pour chaque poste ou serveur Windows avec le service WMI, avec différentes configurations de rapports pour mettre en valeur différents aspects du déploiement.

Les données recueillies à distance fourniront aux responsables IT des rapports d'audit et d'inventaire à la demande, toujours actualisés, accompagnés de rapports sur la sécurité de l'entreprise.

3. ASSURER LA CONFORMITÉ AVEC LES LICENCES LOGICIELLES ET IDENTIFIER LES APPLICATIONS NON AUTORISÉES

Les applications non autorisées et « rogues » installées ou exécutées par les utilisateurs qui les ont téléchargées sur Internet sont un risque de sécurité constant pour la plupart des administrateurs réseau. Nombre de ces applications passent inaperçues jusqu'à ce que le fonctionnement de l'entreprise soit menacé, par une panne du réseau provoquée par un important trafic inconnu, ou jusqu'à ce qu'on détecte la compromission des systèmes du réseau. De nombreux employés utilisant ces applications rogues n'ont pas conscience du risque de sécurité qu'ils font courir à leur entreprise. Les applications rogues peuvent exploiter du code malveillant dans le réseau de l'entreprise et transmettre des données confidentielles à des cybercriminels.

Grâce à la visibilité complète de tous les logiciels du réseau d'une entreprise compatibles avec Windows, les administrateurs peuvent surveiller de façon proactive les logiciels achetés légalement et les applications non autorisées, ce qui peut servir de preuve lors d'un audit financier et réduit le risque de poursuite ou de problèmes judiciaires liés aux applications non autorisées, piratées.

4. RÉDUIRE LES COÛTS LIÉS À L'ADMINISTRATION D'UN SYSTÈME D'INVENTAIRE SÉPARÉ ET D'AGENTS SUR LES POSTES DE TRAVAIL

Les Petites et Moyennes Entreprises profitent directement de l'intégration de l'administration antimalware et réseau de Bitdefender car elles ont ainsi moins besoin d'applications spécialisées et d'agents déployés sur les stations de travail et les serveurs du réseau.

La fonction d'audit utilisée par WMI ne nécessite par d'agent d'inventaire sur le poste de travail, et a donc un impact minime sur la mémoire et les performances système de chaque poste de travail lors du processus programmé de recueil de données.

5. IDENTIFIER LE MATÉRIEL/LES LOGICIELS NE RÉPONDANT PAS À LA CONFIGURATION MINIMALE REQUISE PAR LA POLITIQUE DE L'ORGANISATION

Les rapports d'audit peuvent fournir des rapports encore plus personnalisés afin de répondre à des besoins spécifiques basés sur une liste prédéfinie de critères matériels ou logiciels.

Ces derniers peuvent consister à identifier le matériel à remplacer, à mettre à niveau de la mémoire physique pour répondre aux besoins des applications, ou simplement à vérifier que toutes les stations de travail ont suffisamment d'espace disque libre.

Il est également facile d'identifier des logiciels dans le réseau en faisant une requête par nom et version de l'application (par exemple Microsoft Office ou Outlook). On peut aisément détecter et signaler les stations de travail sur lesquelles certaines applications sont installées en définissant des critères de requête logiciels.

4. PRÉSENTATION DE L'AUDIT RÉSEAU DE BITDEFENDER

La fonctionnalité d'audit réseau de la console d'administration de Bitdefender exploite les scripts WMI intégrés pour permettre aux administrateurs informatiques de créer des aperçus de la configuration logicielle et matérielle des systèmes Windows du réseau. Les informations recueillies à distance fournissent aux responsables IT des rapports d'audit et d'inventaire à la demande, toujours actualisés, accompagnés de rapports sur la sécurité globale de l'entreprise.

Cette section explique comment la fonctionnalité d'audit réseau de Bitdefender recueille les données d'audit du réseau de l'entreprise et génère quatre types de rapports différents, directement à partir des données collectées ou à partir de la base de données.

1. **L'assistant de rapports Snapshot** permet d'afficher la configuration des logiciels et du matériel

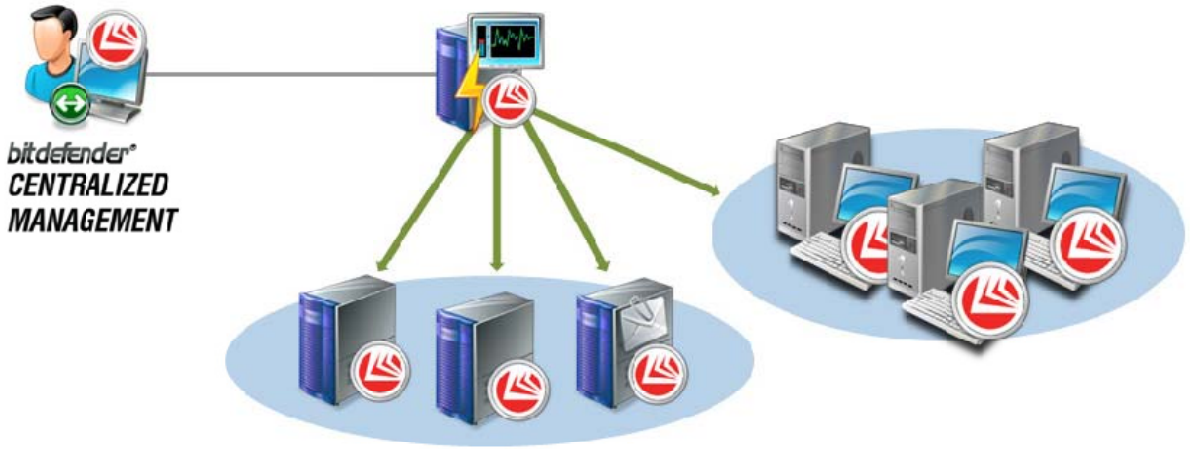
2. **L'assistant des rapports chronologiques** permet de suivre l'historique des installations et des désinstallations de logiciels sur le réseau (au cours d'une période donnée) pour une visibilité complète des changements une fois la période définie.

3. Les **rapports comparatifs** comparent les logiciels installés ou désinstallés dans le réseau à deux moments différents, avec des informations chronologiques pour faciliter la gestion des changements. En raison des paramètres requis pour le rapport comparatif, celui-ci ne peut pas être généré automatiquement et envoyé à une fréquence prédéfinie.

4. **Les rapports personnalisés** contiennent tous les paramètres les plus courants concernant : le type et la vitesse du processeur ; les lecteurs de disques ; le système de fichiers et l'espace disponible restant ; le système d'exploitation et les Service Packs spécifiques ; le fabricant des cartes mères, le numéro de série et la version ; la taille et l'emplacement du fichier de la page de mémoire virtuelle, la mémoire physique ; les logiciels installés par nom et version (par exemple, Microsoft Office ou Outlook).

5. COLLECTER DES DONNÉES D'AUDIT RÉSEAU

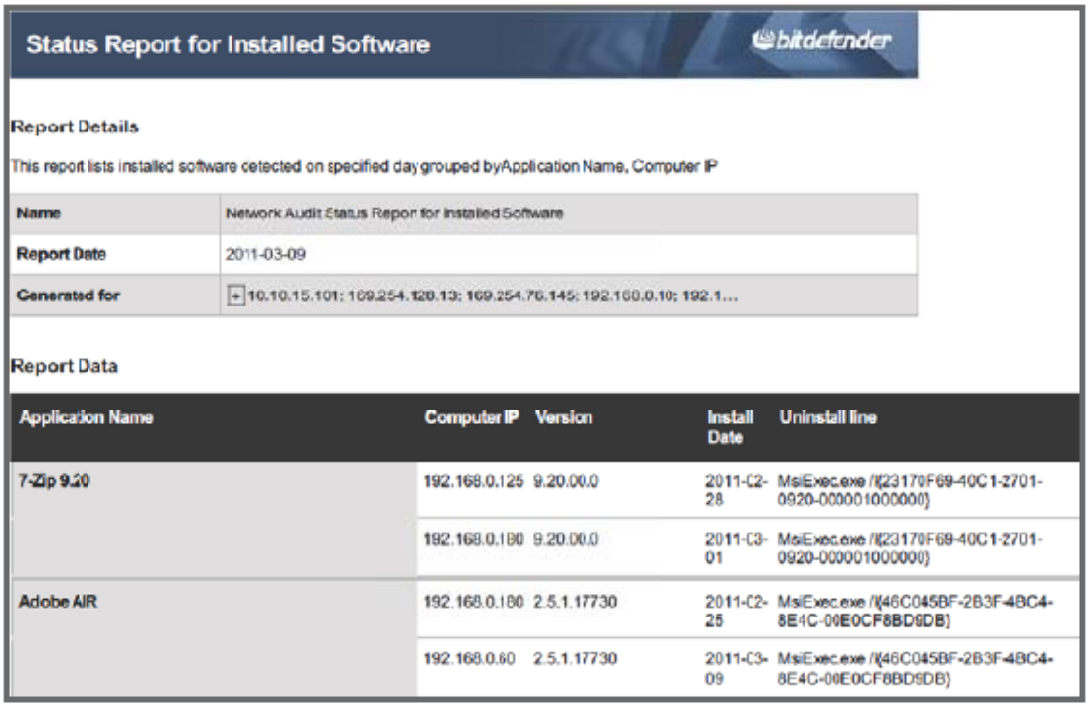
Avant que la fonctionnalité d'audit réseau ne puisse être utilisée pour les rapports d'audit, elle doit être configurée afin de recueillir les données d'audit à partir des systèmes Windows déployés dans le réseau. Les rapports Snapshot peuvent recueillir rapidement des données et l'évolution peut être surveillée pendant le processus de collecte des données avec des informations sur le nombre de stations de travail intégrées. Pour une performance optimisée dans des réseaux plus importants, les rapports d'audit ne peuvent pas être générés à l'aide de données en temps réel du réseau ; celles-ci doivent être collectées dans la base de données d'audit du serveur d'administration avant la création des rapports.



Une fois les données initiales recueillies, le collecteur de données peut être configuré pour s'exécuter tous les jours – ou moins souvent sur les réseaux plus petits – afin d'actualiser les informations logicielles et matérielles dans la base de données d'audit du serveur d'administration. Les aperçus d'audit logiciel sont conservés pour les rapports chronologiques des modifications afin de connaître tous les logiciels du réseau installés ou désinstallés (au cours d'une période donnée). Les informations sur le matériel peuvent être indiquées pour l'état de l'aperçu en cours, mais pas en tant que rapports historiques.

Les administrateurs ont également la possibilité d'archiver les données d'audit sur un périphérique local ou distant à des fins de reporting chronologique, afin que la base de données d'audit soit légère et plus réactive lors de la génération de rapports.

5.1 L'ASSISTANT DES RAPPORTS SNAPSHOT



Status Report for Installed Software

bitdefender

Report Details

This report lists installed software detected on specified day grouped byApplication Name, Computer IP

Name	Network Audit Status Repor for Installed Software
Report Date	2011-03-09
Generated for	10.10.15.101; 169.254.120.13; 169.254.76.145; 192.168.0.10; 192.1...

Report Data

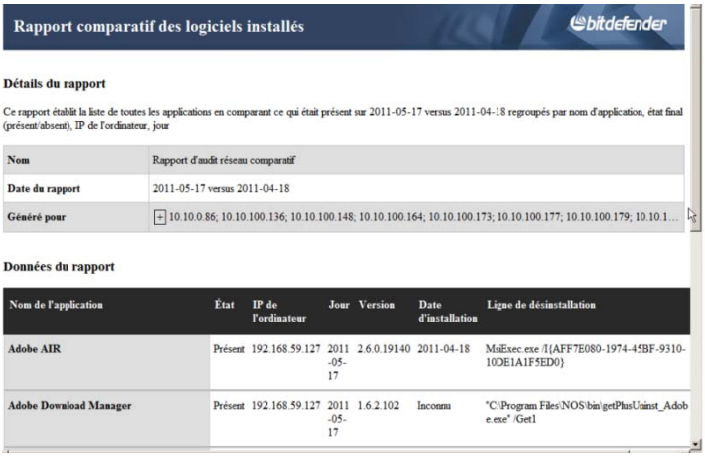
Application Name	Computer IP	Version	Install Date	Uninstall line
7-Zip 9.20	192.168.0.125	9.20.00.0	2011-02-28	MsiExec.exe /I{23170F69-40C1-2701-0920-000001000000}
	192.168.0.180	9.20.00.0	2011-03-01	MsiExec.exe /I{23170F69-40C1-2701-0920-000001000000}
Adobe AIR	192.168.0.180	2.5.1.17730	2011-02-25	MsiExec.exe /I{46C045BF-2B3F-4BC4-8E4C-00E0CF8BD9DB}
	192.168.0.60	2.5.1.17730	2011-03-09	MsiExec.exe /I{46C045BF-2B3F-4BC4-8E4C-00E0CF8BD9DB}

Les rapports Snapshot sont utilisés pour afficher la configuration logicielle et matérielle de postes de travail ou de groupes de systèmes déployés dans le réseau. Le rapport peut être généré pour un rapport spécifique, prédéfini, comme le rapport Système d'exploitation de l'exemple ci-dessous.

5.2 L'ASSISTANT DES RAPPORTS CHRONOLOGIQUES

Les rapports chronologiques sont utilisés pour générer des rapports pour du matériel ou des logiciels installés ou désinstallés avec des informations regroupées par ordinateur (IP), nom d'application ou changement effectué (par exemple, installation ou désinstallation d'une application).

Le rapport



Rapport comparatif des logiciels installés

bitdefender

Détails du rapport

Ce rapport établit la liste de toutes les applications en comparant ce qui était présent sur 2011-05-17 versus 2011-04-18 regroupés par nom d'application, état final (présent/absent), IP de l'ordinateur, jour

Nom	Rapport d'audit réseau comparatif
Date du rapport	2011-05-17 versus 2011-04-18
Généré pour	10.10.0.86; 10.10.100.136; 10.10.100.148; 10.10.100.164; 10.10.100.173; 10.10.100.177; 10.10.100.179; 10.10.1...

Données du rapport

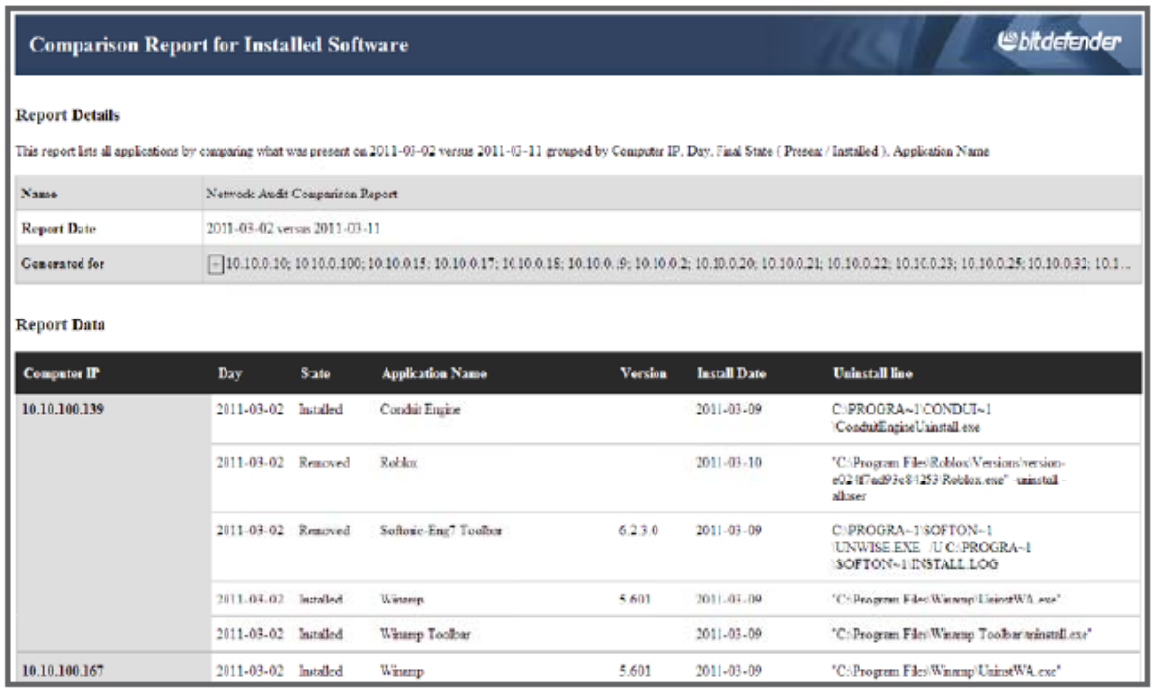
Nom de l'application	État	IP de l'ordinateur	Jour	Version	Date d'installation	Ligne de désinstallation
Adobe AIR	Présent	192.168.59.127	2011-05-17	2.6.0.19140	2011-04-18	MsiExec.exe /I{AFF7E080-1974-45BF-9310-10DE1A1F5ED0}
Adobe Download Manager	Présent	192.168.59.127	2011-05-17	1.6.2.102	Inconnu	"C:\Program Files\NOS\bin\getPlusUninst_Adobe.exe" /Get1

d'exemple ci-dessous a

été généré pour regrouper les données d'audit en fonction d'une adresse IP et les actions effectuées sur ce système. Le rapport peut être utilisé pour voir les applications installées tous les mois et prendre les actions nécessaires pour identifier et désinstaller les fausses applications ou les applications non autorisées du réseau de l'entreprise. De nombreuses organisations doivent suivre les modifications logicielles et générer des rapports afin de respecter la politique de sécurité interne ou leurs obligations légales. Les informations contenues dans le rapport doivent donc être suffisamment précises pour identifier la version spécifique des applications et les postes de travail sur lesquels elles ont été installées pendant la période couverte par le rapport.

5.3 L'ASSISTANT DES RAPPORTS COMPARATIFS

Les rapports comparatifs sont créés à l'aide d'un assistant, peuvent servir à mettre en évidence les modifications effectuées entre deux moments et peuvent être regroupés par ordinateur (IP), nom d'application ou modification appliquée (par exemple, l'installation ou la désinstallation d'une application). Le rapport d'exemple ci-dessous a été généré afin de regrouper les données d'audit par ordinateur (IP).



Comparison Report for Installed Software

Report Details

This report lists all applications by comparing what was present on 2011-03-02 versus 2011-03-11 grouped by Computer IP, Day, Final State (Present / Installed), Application Name

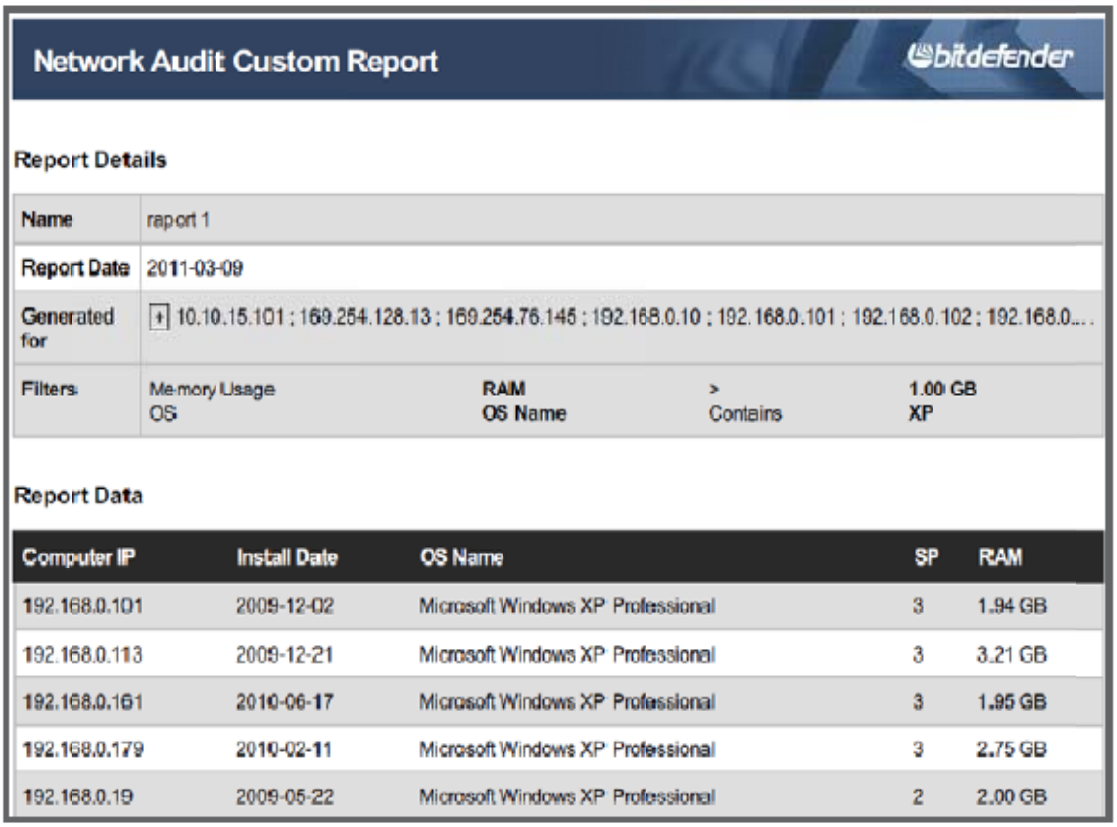
Name	Network Audit Comparison Report
Report Date	2011-03-02 versus 2011-03-11
Generated for	10.10.0.10; 10.10.0.100; 10.10.0.15; 10.10.0.17; 10.10.0.18; 10.10.0.9; 10.10.0.2; 10.10.0.20; 10.10.0.21; 10.10.0.22; 10.10.0.23; 10.10.0.25; 10.10.0.31; 10.1...

Report Data

Computer IP	Day	State	Application Name	Version	Install Date	Uninstall line
10.10.100.139	2011-03-02	Installed	Conduit Engine		2011-03-09	C:\PROGRA~1\CONDUI~1\ConduitEngineUninstall.exe
	2011-03-02	Removed	Roblox		2011-03-10	"C:\Program Files\Roblox\Versions\version-e02f87ad93e81253\Roblox.exe" -uninstall -alluser
	2011-03-02	Removed	Softonic-Eng7 Toolbar	6.2.3.0	2011-03-09	C:\PROGRA~1\SOFTON~1\UNWISE.EXE /U C:\PROGRA~1\SOFTON~1\INSTALL.LOG
	2011-03-02	Installed	Winamp	5.601	2011-03-09	"C:\Program Files\Winamp\UninstWA.exe"
	2011-03-02	Installed	Winamp Toolbar		2011-03-09	"C:\Program Files\Winamp Toolbar\uninstall.exe"
10.10.100.167	2011-03-02	Installed	Winamp	5.601	2011-03-09	"C:\Program Files\Winamp\UninstWA.exe"

5.4 L'ASSISTANT DES RAPPORTS PERSONNALISÉS BASÉS SUR DES REQUÊTES

L'assistant des rapports personnalisés est utilisé pour définir une requête afin d'obtenir des rapports contenant certains paramètres logiciels ou matériels. La requête peut comprendre un ou plusieurs paramètres les plus courants concernant : le type de processeur, sa vitesse, les processeurs monocœurs/à double cœur, les lecteurs de disques, le système de fichiers et l'espace disponible restant, le système d'exploitation et les Service Packs spécifiques, le fabricant des cartes mères, le numéro de série et la version, la taille et l'emplacement du fichier de la page de mémoire virtuelle, la mémoire physique, les logiciels installés par nom et version (par exemple, Microsoft Office ou Outlook). Le rapport d'exemple ci-dessous a été généré pour une utilisation de la mémoire RAM supérieure à 1 000 Mo (1 Go). Ces informations ont permis d'identifier les ordinateurs avec suffisamment de mémoire pour installer un nouveau système d'exploitation, ou pour exécuter des applications requérant au moins 1 Go de mémoire RAM.



Network Audit Custom Report

Report Details

Name	raport 1				
Report Date	2011-03-09				
Generated for	10.10.15.101 ; 169.254.128.13 ; 169.254.76.145 ; 192.168.0.10 ; 192.168.0.101 ; 192.168.0.102 ; 192.168.0....				
Filters	Memory Usage OS	**RAM** **OS Name**	> Contains	**1.00 GB** **XP**	

Report Data

Computer IP	Install Date	OS Name	SP	RAM
192.168.0.101	2009-12-02	Microsoft Windows XP Professional	3	1.94 GB
192.168.0.113	2009-12-21	Microsoft Windows XP Professional	3	3.21 GB
192.168.0.161	2010-06-17	Microsoft Windows XP Professional	3	1.95 GB
192.168.0.179	2010-02-11	Microsoft Windows XP Professional	3	2.75 GB
192.168.0.19	2009-05-22	Microsoft Windows XP Professional	2	2.00 GB

6. PRÉSENTATION DES TÂCHES RÉSEAU DE BITDEFENDER

La gestion de la sécurité et du réseau peut être réalisée plus efficacement à partir d'une seule interface en utilisant la Console d'administration de Bitdefender.

Cette fonctionnalité intégrée permet aux administrateurs informatiques de passer moins de temps à effectuer des tâches fastidieuses en centralisant les tâches d'administration basiques de Windows pour les stations de travail et les serveurs déployés dans le réseau.

Le personnel du service informatique peut être plus efficace avec moins de ressources grâce à l'interface de Bitdefender avec assistant permettant d'automatiser la planification et l'exécution de tâches lancées sur les groupes de systèmes. Le serveur d'administration s'intègre également à Active Directory et permet une administration simple et flexible, sans avoir besoin de recréer la structure des utilisateurs et des groupes déjà présente dans le réseau.

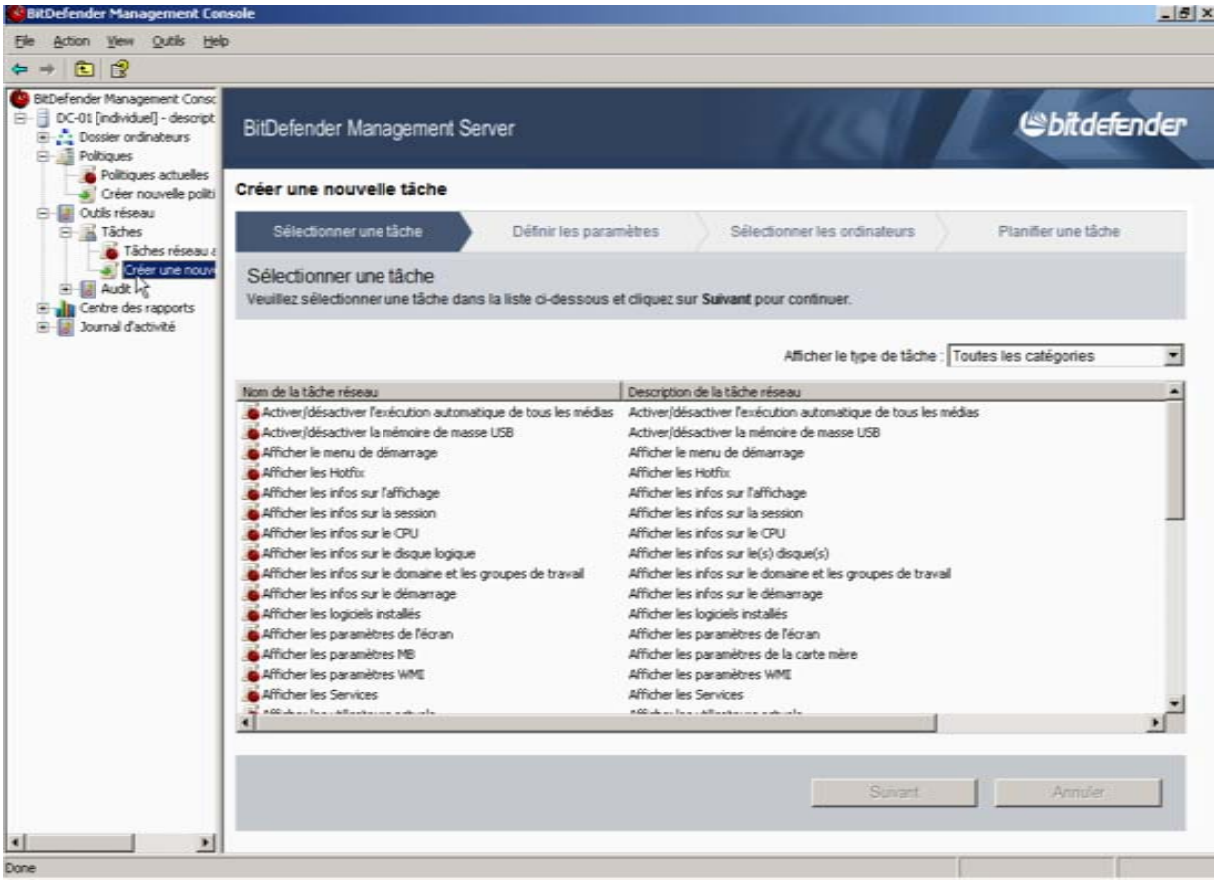
Les tâches réseau de la Console d'Administration peuvent réduire les efforts administratifs en permettant au personnel informatique d'effectuer une action directement (comme désinstaller des logiciels, redémarrer ou éteindre un système, et déconnecter des utilisateurs) sans avoir besoin d'accéder physiquement au système. Les tâches réseau contribuent également à rendre les systèmes plus sûrs et conformes aux politiques de sécurité en modifiant à distance les configurations système et en verrouillant certaines configurations – en désactivant la fonction autorun de Windows et en limitant l'utilisation de périphériques de stockage USB sur le réseau.

Enfin, trois exemples de tâches d'administration réseau sont présentés en détail pour montrer ce qui peut être effectué à l'aide de Bitdefender :

1. Collecte d'informations concernant les postes Windows (serveurs ou stations de travail)
2. Visibilité et Contrôle des applications
3. Renforcement de la sécurité de votre réseau

6.1 EXÉCUTION DE TÂCHES RÉSEAU AVEC ASSISTANT

Les administrateurs informatiques peuvent exécuter des tâches de la section Tâches réseau de la Console d'Administration Bitdefender.



Tâches réseau avec assistant dans la Console d'Administration

Les tâches peuvent être exécutées sur tout poste de travail géré par Bitdefender Management Server.

Voici comment procéder pour créer et exécuter des scripts :

1. Dans la console d'administration, l'administrateur informatique crée une tâche à l'aide du modèle de tâche adapté à la tâche à exécuter. Dans la plupart des cas, le script est créé immédiatement, sans rien avoir à configurer.

2. L'administrateur informatique affecte la tâche à exécuter sur certains postes de travail clients ou groupes de postes de travail clients. Le script peut être programmé pour être exécuté une fois seulement, ou régulièrement.

3. Lors de la session de communication agent-serveur, Bitdefender Management Server envoie la demande de requête à Bitdefender Management Agent installé sur les postes de travail clients concernés.

4. Bitdefender Management Agent exécute le script immédiatement ou selon la planification.

5. Une fois le script exécuté, Bitdefender Management Agent envoie les résultats à Bitdefender Management Server.

6. L'administrateur informatique peut vérifier les résultats dans la console d'administration.

6.2 MODÈLES DE TÂCHES RÉSEAU

Bitdefender permet de créer des tâches réseau à partir de modèles prédéfinis basés sur des tâches écrites à l'avance et testées. Le tableau ci-dessous présente les 37 modèles de tâches réseau disponibles, regroupés en fonction de leur utilisation :

Tâches réseau prédéfinies disponibles dans v3.5

Actions administratives *12 modèles de tâches*	Informations sur les systèmes et logiciels *15 modèles de scripts*	Informations sur le disque et le matériel *10 modèles de scripts*
edémarrer un ordinateur	ystème d'exploitation	artages actuels
teindre un ordinateur	btenir des infos système	space disque disponible
ctiver/désactiver Autorun	echercher le dernier Service Pack installé	fficher les infos sur le disque logique
ctiver/désactiver le stockage de masse USB	fficher les programmes de démarrage	numération de la mémoire
nstaller les mises à jour de Windows	fficher les logiciels installés	numération de la mémoire
erminer un processus	fficher les correctifs	rtuelle
ermer la session de l'utilisateur	fficher les processus en cours	fficher les infos sur le processeur
onnexion Bureau à Distance	fficher les services	fficher les paramètres de la carte mère
ésinstaller un logiciel	fficher les paramètres WMI	fficher les infos vidéo
xécuter un programme	fficher les infos sur le démarrage	fficher les paramètres du moniteur
nvoyer un message	fficher le menu de démarrage	fficher les valeurs de la carte réseau
Mises à jour automatiques Windows	fficher les utilisateurs actuels	
	fficher les utilisateurs locaux	
	fficher les infos sur le domaine et les groupes de travail	
	fficher les infos sur la session	

6.3 EXEMPLE 1 : COLLECTER DES INFORMATIONS SUR LES POSTES DE TRAVAIL

Les tâches peuvent être utilisées pour résoudre certains problèmes. L'administrateur informatique peut exécuter à distance certaines tâches pour obtenir des informations préliminaires sur les stations de travail clientes présentant des problèmes. Ces informations lui permettent de mieux cerner les problèmes et de trouver des solutions potentielles rapidement.

Le script **Obtenir les infos système**, par exemple, fournit des informations utiles sur les stations de travail clientes telles que :

- Des informations sur le système d'exploitation
- Le nom, le modèle et le fabricant du système

- La mémoire RAM totale
- Le processeur
- La version du BIOS

Le script « Obtenir des infos système » fournit des informations précieuses sur chaque station de travail

6.4 EXEMPLE 2 : CONTRÔLE DES APPLICATIONS SUR LES STATIONS DE TRAVAIL

Certaines tâches aident à assurer la conformité avec les politiques de l'entreprise concernant l'utilisation des applications. En utilisant uniquement Bitdefender Management Console, l'administrateur informatique peut facilement savoir quels logiciels sont installés sur les stations de travail clientes et désinstaller les applications indésirables.

ÉTAPE 1 – VÉRIFIER LES APPLICATIONS INSTALLÉES

Pour vérifier les applications installées sur les stations de travail clientes, l'administrateur informatique peut utiliser la tâcher « Lister les logiciels installés ». Cette tâche peut servir à obtenir la liste des applications installées sur les stations de travail clientes, y compris les mises à jour Microsoft et Windows.

Une fois la tâche exécutée, l'administrateur informatique peut vérifier les résultats dans le panneau « Tâches réseau actuelles » en double-cliquant sur la tâche. L'image ci-dessous fournit un exemple des résultats collectés pour une station de travail cliente.

7.	*Name:* Microsoft Internationalized Domain Names Mitigation APIs *Description:* Microsoft Internationalized Domain Names Mitigation APIs *Uninstall command line:* N/A	N/A	2010-03-01
8.	*Name:* Windows Internet Explorer 7 *Description:* Windows Internet Explorer 7 *Uninstall command line:* N/A	20070813.165237	2010-03-01
9.	*Name:* Security Update for Windows XP (KB2079403) *Description:* Security Update for Windows XP (KB2079403) *Uninstall command line:* N/A	1	2010-08-11
10.	*Name:* Security Update for Windows XP (KB2115168) *Description:* Security Update for Windows XP (KB2115168) *Uninstall command line:* N/A	1	2010-08-11
11.	*Name:* Security Update for Windows XP (KB2121546) *Description:* Security Update for Windows XP (KB2121546) *Uninstall command line:* N/A	1	2010-09-16
12.	*Name:* Update for Windows XP (KB2141007) *Description:* Update for Windows XP (KB2141007) *Uninstall command line:* N/A	1	2010-09-16
13.	*Name:* Hotfix for Windows XP (KB2158563) *Description:* Hotfix for Windows XP (KB2158563) *Uninstall command line:* N/A	1	2010-09-30
14.	*Name:* Security Update for Windows XP (KB2160329) *Description:* Security Update for Windows XP (KB2160329) *Uninstall command line:* N/A	1	2010-08-11
15.	*Name:* Security Update for Windows Internet Explorer 7 (KB2183461)	1	2010-08-11

Exemple de liste des logiciels installés détectés sur une station de travail

CONSEIL : AUTRES SCRIPTS UTILES

Deux autres scripts peuvent fournir des informations supplémentaires au sujet des logiciels installés sur les stations de travail clientes :

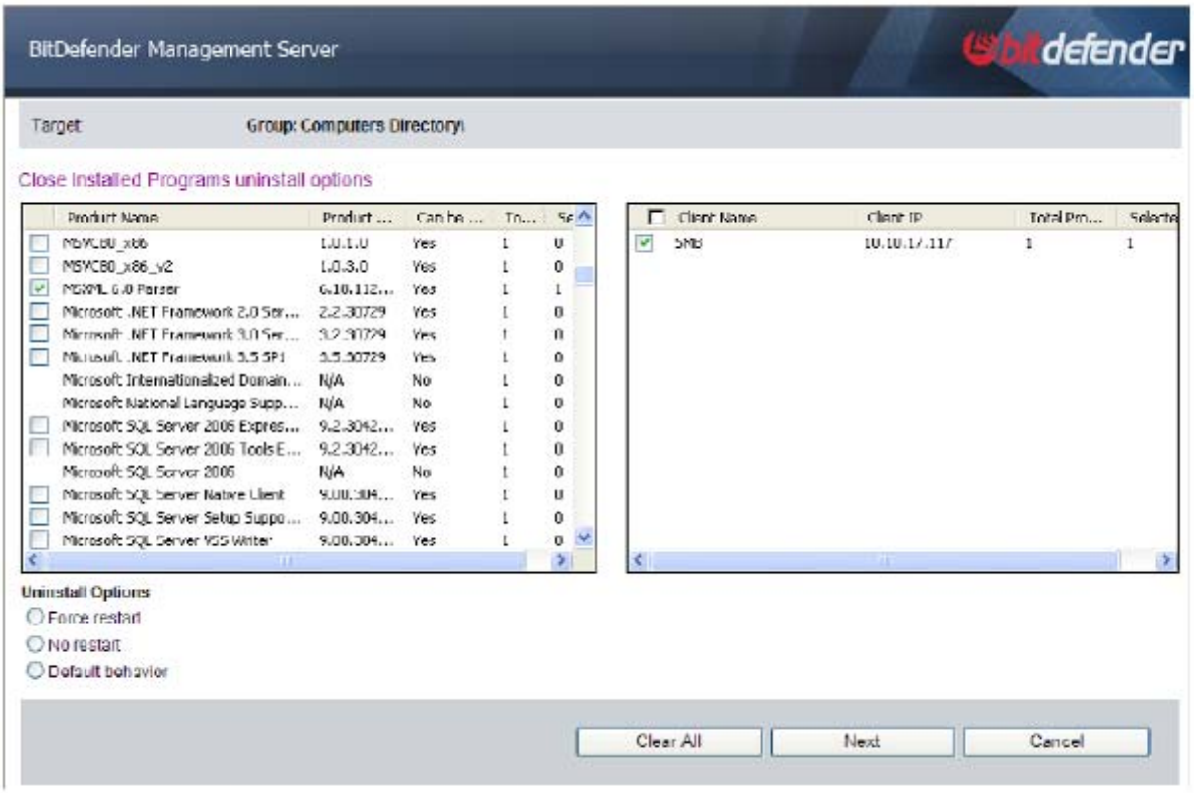
- *« Afficher le menu de démarrage » indique les applications ayant des raccourcis dans le menu « Démarrer »*
- *« Processus en cours » fournit des informations sur les processus en cours d'exécution sur les stations de travail clientes.*

ÉTAPE 2 – DÉSINSTALLER DES APPLICATIONS

Si une application installée sur une station de travail cliente ne respecte pas les politiques d'utilisation des applications, elle peut facilement être désinstallée à partir de la section résultats de la tâche « Afficher les logiciels installés ». Voici quelques exemples de types d'applications pouvant être désinstallés à distance :

- Solutions antivirus tierces
- Applications voIP et de chat
- Peer to peer
- Multimédia et jeux

Pour désinstaller une application, l'administrateur informatique doit cliquer sur le lien au-dessus du tableau des résultats.



Exemple de programmes sélectionnés pour être désinstallés

Deux tableaux apparaissent ici :

- Le tableau de gauche indique toutes les applications installées sur les stations de travail clientes sur lesquelles le script a été exécuté.
- Le tableau de droite indique toutes les stations de travail clientes sur lesquelles une application sélectionnée est installée.

Vous pouvez désinstaller une application indésirable facilement en quelques étapes :

1. Sélectionnez l'application dans la liste.
2. Si vous souhaitez supprimer l'application sur toutes les stations de travail qui la contiennent, sélectionnez la case à cocher dans l'en-tête de la colonne « Nom du client ». Si vous souhaitez la supprimer seulement sur certaines stations de travail, cochez les cases correspondantes.
3. Sélectionnez une option de redémarrage. Il peut être nécessaire de redémarrer l'ordinateur pour désinstaller complètement l'application sélectionnée.
4. Cliquez sur « Désinstaller » puis sur « OK » pour désinstaller l'application sur les ordinateurs sélectionnés.

Une tâche « Exécuter un programme » est automatiquement créée et affectée aux ordinateurs sélectionnés afin que l'application soit désinstallée. La désinstallation de l'application ne nécessite par d'intervention de l'utilisateur.

Une fois le script exécuté, l'administrateur informatique peut vérifier les résultats afin de voir si le script s'est bien exécuté dans le panneau « Tâche réseau en cours » en double-cliquant sur le script.

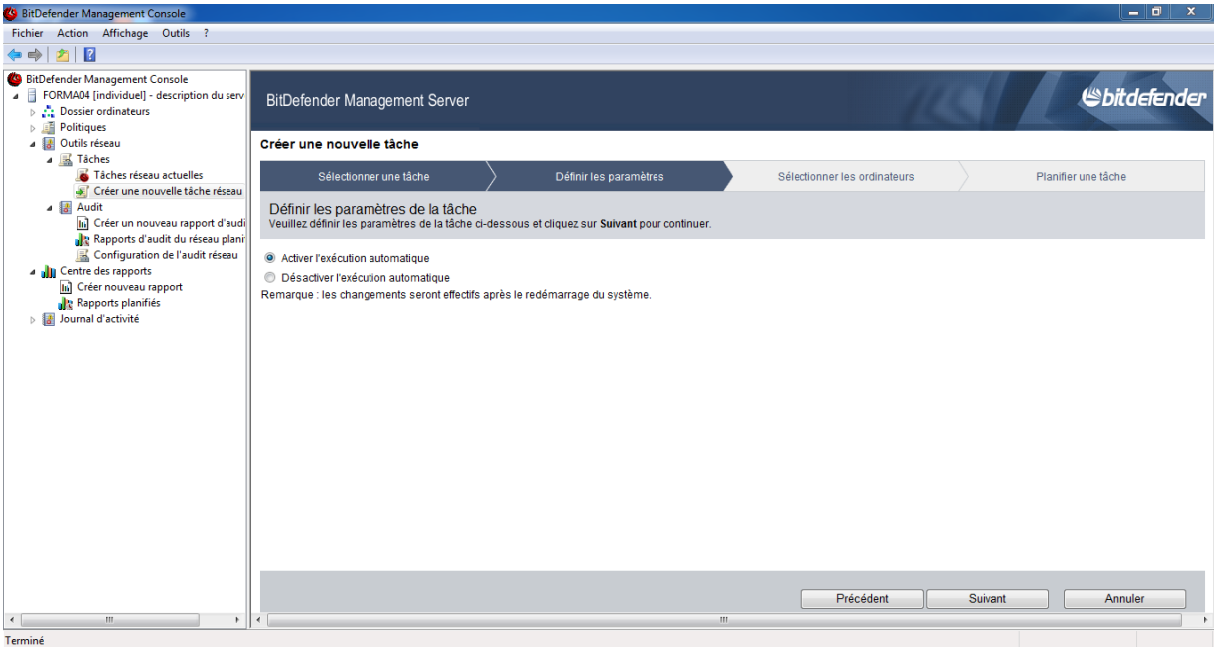
6.5 EXEMPLE 3 : RENFORCER LA SÉCURITÉ DE VOTRE RÉSEAU

Les vers informatiques utilisent de plus en plus les supports de stockage USB et la fonction « Autorun » de Windows pour se diffuser sur les réseaux. C'était le cas du ver Downadup, également connu sous le nom de « Conficker » ou « Kido », qu'on estime être à l'origine de l'infection de millions d'ordinateurs de réseaux d'entreprises.

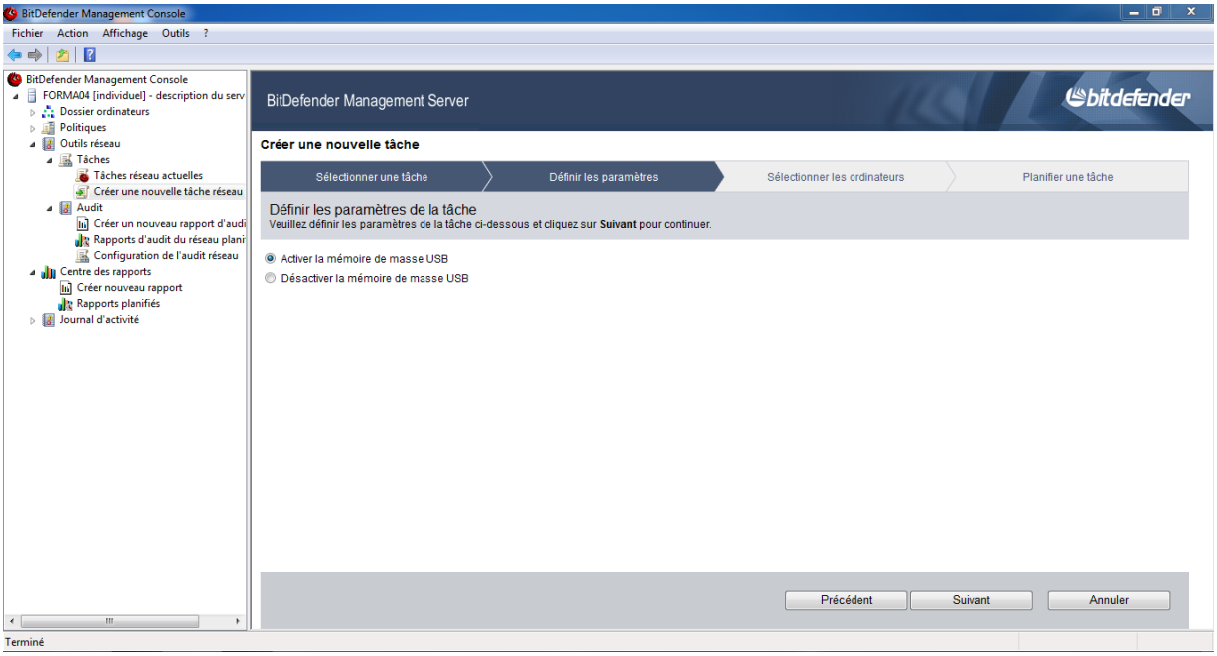
Note : Autorun active la détection et la lecture automatiques de nouveaux supports : clés USB, volumes partagés, CD, DVD et d'autres. Cette fonctionnalité de Windows peut être utilisée pour exécuter automatiquement du code malveillant dès qu'un support infecté est connecté à l'ordinateur.

Pour aider les administrateurs informatiques à lutter contre ces vulnérabilités du réseau, Bitdefender Client Security fournit les tâches suivantes :

- Activer/désactiver l'exécution automatique – pour contrôler à distance l'exécution automatique sur tous les lecteurs des ordinateurs administrés



- Activer/désactiver la mémoire de masse USB – pour autoriser ou bloquer à distance le stockage de masse USB sur les ordinateurs administrés



Les administrateurs informatiques peuvent exécuter ces tâches sur tous les ordinateurs administrés pour désactiver complètement la fonction autorun et les périphériques de stockage USB du réseau. Ces tâches peuvent ensuite être exécutées en fonction des besoins pour désactiver temporairement la fonction autorun et les périphériques de stockage USB sur certains ordinateurs ou groupes administrés.

7. CONCLUSION

Dans une même version, qu'il s'agisse de réseaux de sociétés ou PME, Bitdefender associe protection antimalware, audit à distance et administration système, en utilisant la technologie WMI (Windows Management Instrumentation), qui permet aux administrateurs système d'obtenir un gain de visibilité et de protection qui les aide à identifier et à supprimer les brèches existant dans leur réseau. Grâce à un degré de visibilité supérieur et à une administration renforcée, les solutions Business de Bitdefender dépassent les solutions antimalwares traditionnelles pour entreprises et protègent les services cruciaux comme les systèmes de messagerie, les postes de travail et les serveurs, des attaques, qu'elles proviennent de l'extérieur ou de l'intérieur de l'entreprise.

À propos de Bitdefender®

Bitdefender est la société créatrice de l'une des gammes de solutions de sécurité la plus complète et la plus certifiée au niveau international figurant parmi les plus rapides et les plus efficaces du marché. Depuis sa création en 2001, Bitdefender n'a cessé d'élever le niveau et de définir de nouveaux standards en matière de protection proactive. Chaque jour, Bitdefender protège des dizaines de millions de particuliers et de professionnels à travers le monde – en leur garantissant une utilisation sécurisée et sereine de l'univers informatique. Les solutions

Bitdefender sont distribuées dans plus de 100 pays via des partenaires revendeurs et distributeurs hautement qualifiés. Plus d'informations sur Bitdefender et ses solutions de sécurité sont disponibles via le centre de presse. Retrouvez également sur le site www.malwarecity.fr des actualités au sujet des menaces de sécurité qui permettent aux utilisateurs de rester informés des dernières évolutions de la lutte contre les malwares.

À propos des solutions Bitdefender® pour Entreprises

Les entreprises peuvent protéger efficacement leurs clients des malwares en utilisant les capacités de Bitdefender à détecter et à supprimer les menaces connues ou de type « zero-day », à assurer la conformité avec les politiques de sécurité de l'entreprise et à les gérer en utilisant le moins de ressources informatiques possibles. Grâce à un audit réseau et à une administration centralisée des systèmes, les solutions Business de Bitdefender protègent les services cruciaux comme les systèmes de messagerie, les postes de travail multiplateformes, les serveurs et les passerelles.

Simples à déployer et faciles à administrer, les solutions Business Security de Bitdefender procurent une visibilité de la sécurité de l'entreprise, et rationalisent les tâches cruciales d'administration. L'administration centralisée réunit les fonctionnalités antimalwares traditionnelles et des outils réseau, sous forme d'assistants, qui simplifient l'administration du paramétrage à distance et l'audit des postes de travail et serveurs Windows.

Téléchargez les versions d'essai des solutions Bitdefender pour Enterprises sur www.bitdefender.fr/business

ANNEXE : DESCRIPTION DE MODÈLES DE TÂCHES RÉSEAU

Cette annexe fournit une description détaillée des modèles de tâches réseau disponibles.

Redémarrer un ordinateur – Fait redémarrer les stations de travail clientes.

Éteindre un ordinateur – Éteint les stations de travail clientes.

Processus en cours – Fournit des informations sur les processus en cours d'exécution sur les stations de travail clientes.

Partages actuels – Fournit des informations sur les partages présents sur les stations de travail clientes.

Activer/désactiver Autorun pour tous les lecteurs – Active ou désactive la fonction Autorun de Windows sur tous les lecteurs des stations de travail clientes. Autorun active la détection automatique et la lecture des nouveaux médias.

Activer/désactiver le stockage de masse USB – Active ou désactive les périphériques de stockage USB sur les stations de travail clientes. Ces périphériques comprennent les clés USB et les lecteurs MP3.

Afficher les programmes de démarrage – Fournit des informations sur tous les programmes qui s'exécutent sur les stations de travail clientes au démarrage.

Énumération de la mémoire (physique RAM) – Indique la quantité de mémoire physique (RAM) présente sur les stations de travail clientes.

Énumération de Pagefile (mémoire virtuelle) – Fournit des informations sur la mémoire virtuelle (pagefile) disponible sur les stations de travail clientes, comprenant l'emplacement et la taille du fichier page file, et la taille initiale/maximale.

Afficher les programmes de démarrage – Fournit des informations sur les programmes installés à l'aide de Windows Installer s'exécutant sur les stations de travail au démarrage.

Espace disque disponible – Fournit la liste des disques logiques sur les stations de travail clientes et l'espace disque disponible sur chacun d'entre eux.

Rechercher le dernier Service Pack installé – Fournit la version du Service Pack de Windows installée sur les stations de travail clientes.

Obtenir des infos système – Fournit des informations sur les stations de travail clientes y compris : des informations sur le système d'exploitation, le nom du système, le modèle et le fabricant, le mémoire RAM totale, le processeur, la version du BIOS.

Installer les mises à jour de Windows – Vous aide à identifier les mises à jour Windows disponibles pour les stations de travail clientes et à installer toutes ou certaines des mises à jour Windows sur les stations de travail clientes.

Terminer un processus – Termine un processus spécifique s'exécutant sur les stations de travail clientes. Le script « Processus en cours » peut être utilisé pour obtenir la liste des processus en cours d'exécution.

Afficher les infos sur le processeur – Fournit des détails sur le processeur des stations de travail clientes y compris : le nom et l'identifiant du processeur, la description, le fabricant, la fréquence d'horloge.

Afficher les utilisateurs actuels – Affiche les utilisateurs connectés aux stations de travail.

Afficher les infos sur le domaine et les groupes de travail – Fournit des informations sur le domaine ou le groupe de travail dont les stations de travail clientes font partie.

Afficher les correctifs – Fournit des informations sur les correctifs Microsoft et Windows installés sur les stations de travail clientes.

Afficher les logiciels installés – Fournit la liste de tous les logiciels et mises à jour Microsoft et Windows installés sur les stations de travail clientes. Une ligne de commande de désinstallation est fournie pour chaque application ou mise à jour installée avec Windows Installer. Vous pouvez désinstaller une application en utilisant cette ligne de commande avec le script « Exécuter un programme ».

Afficher les utilisateurs locaux – Fournit des informations sur les comptes d'utilisateurs locaux Windows configurés sur les stations de travail clientes.

Afficher les infos sur le disque logique – Fournit des informations sur les disques logiques (disquettes, disques durs, CD-ROM, etc.) des stations de travail clientes. Cela comprend le nom (étiquette), la description, l'espace disque disponible, la taille.

Afficher les infos sur la session – Fournit des informations concernant les sessions ouvertes sur les stations de travail clientes.

Afficher les paramètres de la carte mère – Fournit des informations sur la carte mère (Mo) des stations de travail clientes notamment le nom, le fabricant et le numéro de série.

Afficher les paramètres du moniteur – Fournit des informations sur le moniteur des stations de travail clientes notamment le type de moniteur, son fabricant et ses dimensions physiques.

Afficher les valeurs de la carte réseau - Fournit des informations détaillées sur les cartes réseau installées sur les stations de travail clientes notamment le type de carte réseau, le fabricant, l'adresse MAC et réseau

Afficher les services – Fournit des informations au sujet des services s'exécutant sur les stations de travail clientes comprenant le nom, le nom d'affichage, l'état (arrêté/en cours d'exécution), le mode de démarrage (automatique/ manuel/ désactivé), la description.

Afficher les infos sur le démarrage – Fournit des informations sur le démarrage des stations de travail clientes.

Afficher le menu de démarrage - Dresse la liste des raccourcis d'applications qui se trouvent dans le menu « Démarrer » des stations de travail clientes. Les entrées sont regroupées par utilisateur.

Afficher les infos vidéo – Fournit différentes informations sur l'affichage vidéo des stations de travail clientes notamment : le nom et le type d'adaptateur vidéo, la mémoire graphique, la résolution, le nom et la version du pilote et les fréquences de rafraîchissement minimale et maximale.

Afficher les paramètres WMI – Fournit des informations sur les paramètres WMI des stations de travail clientes.

Fermer la session de l'utilisateur – Ferme la session de l'utilisateur connecté aux stations de travail clientes.

Système d'exploitation – Fournit des informations utiles sur le système d'exploitation des stations de travail clientes y compris : le système d'exploitation et sa version, l'utilisateur enregistré, le numéro de série et la date d'installation.

Connexion Bureau à Distance – Modifie les paramètres Windows sur les stations de travail clientes afin d'autoriser ou de bloquer les connexions à distance entrantes via la Connexion Bureau à Distance.

Désinstaller un logiciel – Supprime une application spécifique installée sur des stations de travail clientes. Ce script peut être utilisé pour supprimer toute application figurant dans l'applet « Ajout/Suppression de programmes » du Panneau de configuration.

Exécuter un programme – Exécute une application particulière sur des stations de travail clientes. L'application peut se trouver soit sur la station de travail cible, soit sur la machine locale (où Bitdefender Management Console est installé).

Envoyer un message – Envoie un message aux utilisateurs ayant ouvert une session sur des stations de travail clientes. Pour les stations de travail Windows 2000, la tâche utilise la commande net send et requiert que le service de Messagerie instantanée soit démarré (paramètre par défaut). Pour les autres stations de travail Windows, la tâche utilise la commande msg et requiert que le service Terminal Services soit démarré (paramètre par défaut).

Mises à jour automatiques Windows - Configure les mises à jour automatiques de Windows sur les postes clients. Les mises à jour automatiques de Windows permettent aux utilisateurs de maintenir leur système d'exploitation à jour.