Gestión de Scripts WMI con BitDefender CLIENT SECURITY

Libro Blanco

1. Introducción

BitDefender Client Security es una solución de seguridad empresarial robusta y fácil de gestionar que ofrece protección proactiva de última generación frente a virus, spyware, rootkits, spam, phishing y otro tipo de malware. BitDefender Client Security aúna una serie de características que permite la administración automática de una red, incluyendo **scripts WMI** (Windows Management Instrumentation)

WMI es la implementación de Microsoft en la administración empresarial basada en web (WBEM), una iniciativa para establecer estándares de acceso y compartición de la administración de información en una red empresarial. WMI se basa en WBEM y ofrece soporte integrado para un modelo de información común (CIM), datos modelo que describen los objetos existentes en una red administrada.

Básicamente, WMI permite la administración de estaciones de trabajo de Windows a través de scripts. Los scripts WMI sólo pueden ejecutarse en las estaciones de trabajo con los servicios WMI instalados. WMI está preinstalado en Windows Vista, Windows Server 2008, Windows Server 2003, Windows XP, Windows Me, y Windows 2000.

Más Información

Para saber más sobre WMI, por favor, acceda a la sección Windows Management Instrumentation en la página web de Microsoft Developer Network (MSDN)

Habitualmente, la implementación y puesta en marcha de cualquier solución totalmente programada para ejecutarse automáticamente es un proceso arduo y complejo. Para evitar el consumo de tiempo que suponen ciertas tareas a la hora de buscar y desarrollar scripts WMI, BitDefender Client Security ofrece una completa serie de plantillas predefinidas para tales propósitos. BitDefender Client Security permite ejecutar scripts WMI en los grupos de puestos de trabajo de una red y ofrece una lista de posibilidades de reducir el esfuerzo de administración centralizando los resultados. De este modo, los administradores de sistemas pueden ejecutar una **auditoría de red** (recopilando información de los equipos tanto del sistema como del hardware) así como **acciones administrativas** de forma remota.

A diferencia de otras soluciones de seguridad empresariales que incluyen software de terceros para ofrecer soporte de scripts WMI, BitDefender Client Security los integra directamente en su consola de administración. De esta manera, nos encontramos con una solución con un bajo Coste Total de Propiedad (TCO) así como con una completa y fácil solución de administración.

2. Beneficios Principales

Muchos son los beneficios que podrá obtener utilizando los scripts WMI implementados en la consola de administración de BitDefender:

Reducción de costes y carga de trabajo a la hora de administrar una red

- Los administradores de sistemas ahorrarán tiempo de aprendizaje que supone el desarrollo de scripts WMI a través de las 30 plantilla predefinidas.
- Reducción considerable del tiempo invertido en centralizar la información de una auditoría de red para todos los puestos de trabajo.
- Permite la administración de la red y su seguridad desde una sola intefaz a través del uso de la consola de administración de BitDefender.
- Ofrece una completa automatización permitiendo ejecutar los scripts WMI a grupos de equipos de trabajo (el Management Server se integra con el Active Directory para una administración de grupo más fácil y sencilla).
- Mejora de las habilidades de gestión y reducción del esfuerzo de administración, permitiendo a los administradores de sistemas gestionar (desinstalar software, reiniciar, apagar, salir del sistema) las estaciones de la red remotamente.
- Ayuda a reducir el periodo de inactividad de un puesto de trabajo ayudando a los administradores de sistemas a localizar y resolver los procesos con información preliminar sobre las estaciones de trabajo afectadas de la red.
- Ayuda a mantener la conformidad de las políticas de uso de la aplicación permitiendo a los administradores de sistemas el control remoto de las aplicaciones instaladas y los procesos que se estén ejecutando en ese momento en las estaciones de trabajo en red.

Mejora en la monitorización y visibilidad de la red

- Permite la ejecución de una auditoria de red obteniendo:
  - *Información del hardware*
  - *Información sobre el software y el sistema*
  - *Información sobre las cuentas de usuario de Windows*
  - *Información sobre el disco y sistemas de archivo*
- Ofrece un acceso rápido y fácil a información centralizando los resultados de cada script.

3. Disponibilidad de plantillas Script WMI

BitDefender Client Security permite crear Scripts WMI basados en plantillas de Scripts WMI predefinidas. La siguiente tabla muestra 32 de las plantillas de script WMI agrupadas por usos:

Categoría	*Plantillas de Script*
Información del Hardware (6 plantillas)	Listar información de la CPU Listar configuración de placa base Listar información de video Listar configuración del monitor Listar valores de adaptadores de red Listar la información del administrador de energía
Información del software y del sistema (11 plantillas)	Sistema operativo Consultar información del sistema Consultar último SP instalado Listar programas de arranque Listar software instalado Listar Parches Procesos en uso Listar Servicios Listar configuración WMI Listar información de arranque Listar menú de arranque
Información sobre las cuentas de usuario de Windows (4 plantillas)	Listar usuarios existentes Listar usuarios locales Listar Información del Dominio y Grupo de Trabajo Listar información de inicio de sesión
Información sobre el disco y sistemas de archivo (5 plantillas)	Recursos compartidos actuales Espacio libre en disco Mostrar información de discos lógicos Enumera memoria Enumerar archivo de paginación
Acciones administrativas (6 plantillas)	Reinicio del equipo Apagado del equipo Cerrar sesión del usuario Eliminar software Detener proceso Ejecutar programa

Puede encontrar una descripción más detallada de cada plantilla script WMI en el apéndice.

Restricciones del sistema operativo

Para ejecutarlos scripts WMI en Windows Server 2003 o sistemas operativos de 64bit, debe instalar primero **Windows Installer Provider (MSI provider**) cuando no venga preinstalado en las instalaciones por defecto.

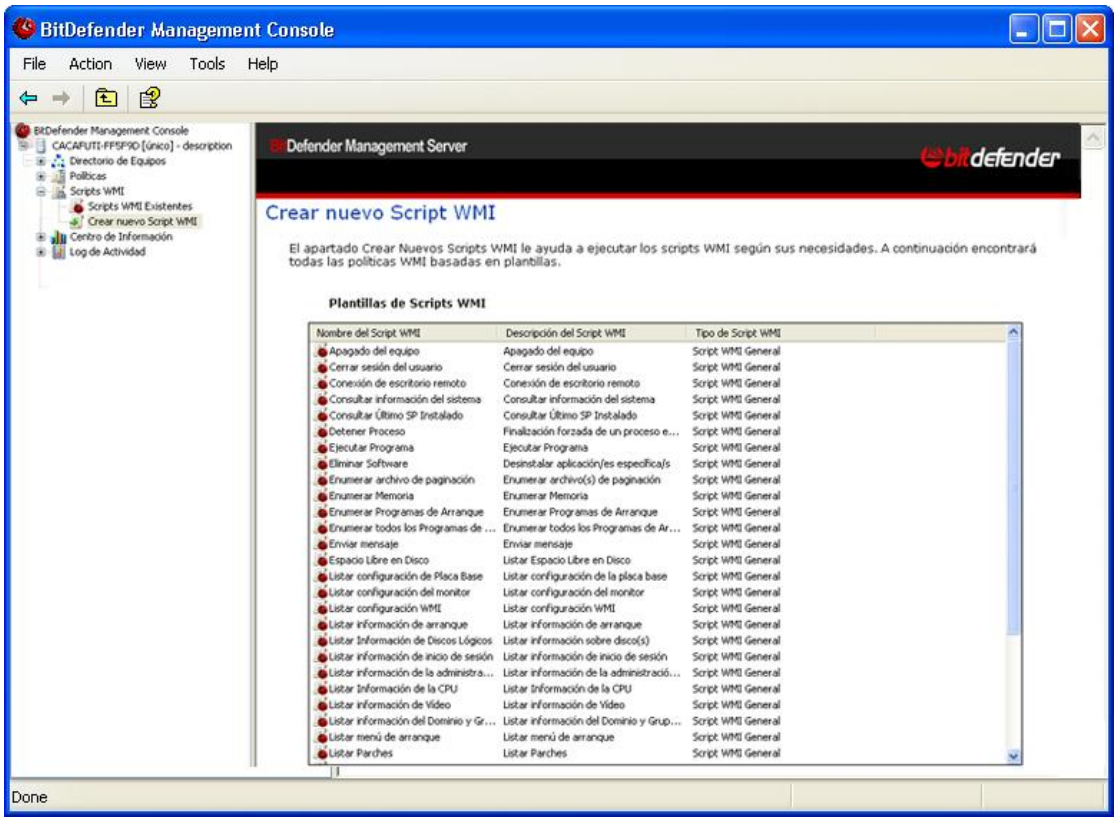
- Enumere programas de arranque
- Liste software instalado
- Obtenga información del sistema

Este proveedor está incluido en el CD de instalación de Windows como componente opcional de Windows y puede instalarse a través del Panel de Control.
Para más información, por favor acceda a los apartados de la página web Microsoft Developer Network (MSDN):

- Operating System Availability of WMI Components
- Windows Installer Provider

4. Funcionamiento

Los administradores de sistemas pueden crean scripts utilizando el complemento dedicado de la consola de administración de BitDefender.



Complemento Scripts WMI

Los scripts WMI pueden ser ejecutados en cualquier puesto administrado mediante la consola de administración de BitDefender.

Aquí encontrará los escenarios de la creación de script y procesos de ejecución:

1. *En la consola de administración, el administrador de redes crea un script WMI utilizando la plantilla de script WMI correspondiente a la tarea a realizar. En la mayoría de los casos, el script es creado inmediatamente, sin tener que configurar ninguna opción.*

2. *El administrador de sistemas asigna el script WMI para que se ejecute en una estación de trabajo específica o un grupo de trabajo. El script puede configurarse para que se ejecute una sola vez o regularmente.*

3. *Durante la sesión de comunicación entre el servidor y el agente, la consola de administración del servidor envía la petición de script al agente instalado en las estaciones de trabajo del cliente asignadas.*

4. *La consola de administración de BitDefender ejecuta el script inmediatamente o cuando esté programado.*

5. *Después del que el script se ejecute, la consola de administración del cliente envía los resultados a la consola de administración del servidor.*

6. *El administrador de sistemas puede analizar los resultados en la consola de administración.*

El siguiente diagrama muestra el funcionamiento de los scripts WMI en BitDefender Client Security

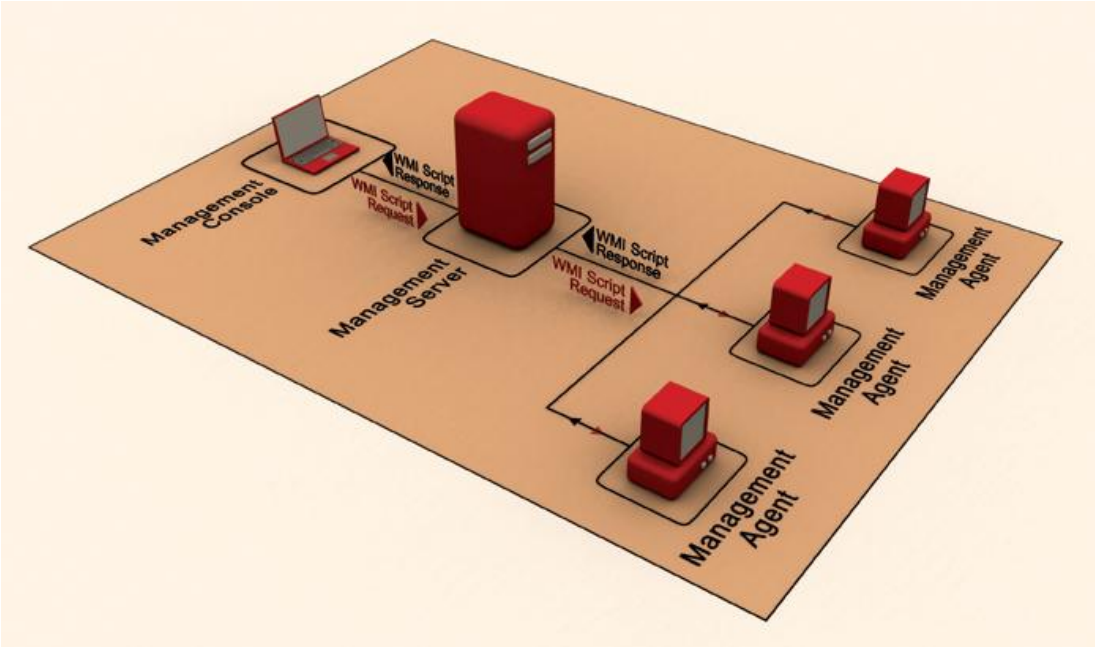


Diagrama de funcionamiento

5. Ejemplos

Aquí ponemos 2 ejemplos de tareas que pueden ser lograrse utilizando los scripts WMI mediante BitDefender Client Security;

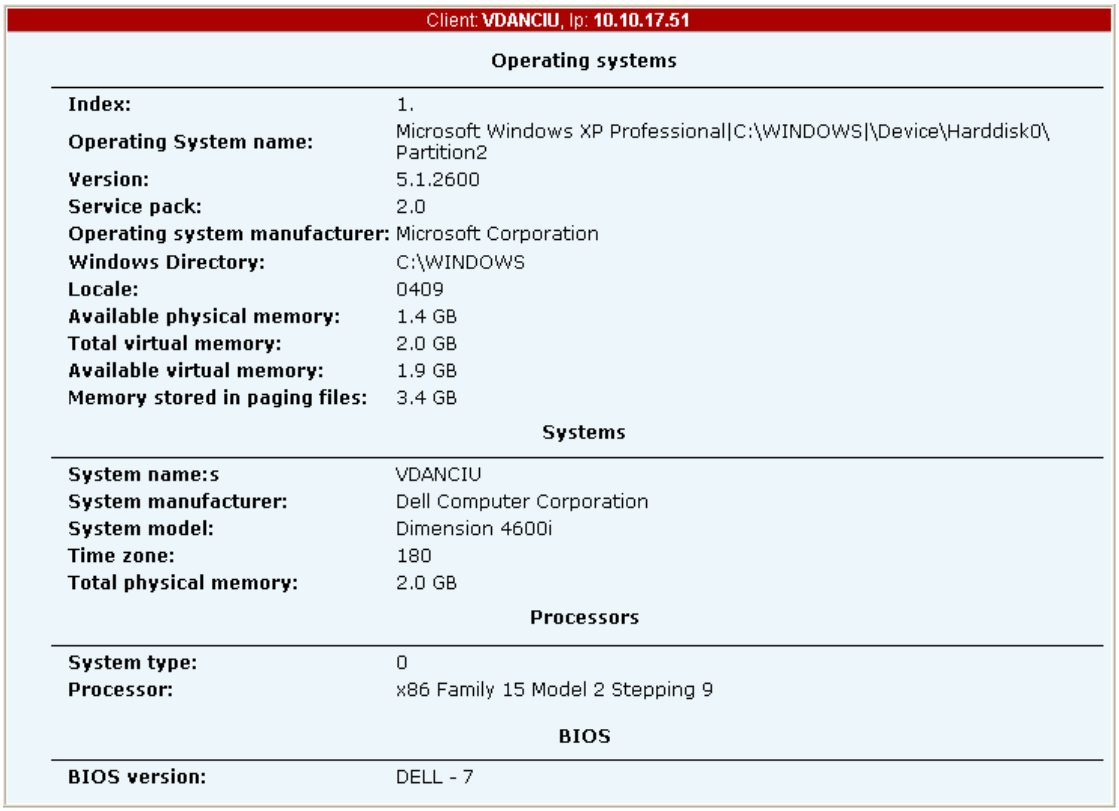
- Recopilar información sobre estaciones de trabajo
- Control de aplicación

5.1. Recopilar información sobre estaciones de trabajo

Los scripts WMI pueden utilizarse para el proceso de localización y resolución de problemas. El administrador de sistemas puede ejecutar remotamente un script WMI para obtener información preliminar del cliente con problemas. Con esta información, el administrador puede evaluar mejor el problema y encontrar soluciones más rápidamente.

El script **Consultar información del sistema**, por ejemplo, ofrece información útil sobre la estación de trabajo sobre:

- Información del sistema operativo
- Nombre del sistema, modelo y fabricante
- Memoria RAM total
- Procesador
- Versión de la BIOS



Client: **VDANCIU**, Ip: **10.10.17.51**

Operating systems

Index:	1.
Operating System name:	Microsoft Windows XP Professional|C:\WINDOWS|\Device\Harddisk0\Partition2
Version:	5.1.2600
Service pack:	2.0
Operating system manufacturer:	Microsoft Corporation
Windows Directory:	C:\WINDOWS
Locale:	0409
Available physical memory:	1.4 GB
Total virtual memory:	2.0 GB
Available virtual memory:	1.9 GB
Memory stored in paging files:	3.4 GB

Systems

System name:s	VDANCIU
System manufacturer:	Dell Computer Corporation
System model:	Dimension 4600i
Time zone:	180
Total physical memory:	2.0 GB

Processors

System type:	0
Processor:	x86 Family 15 Model 2 Stepping 9

BIOS

BIOS version:	DELL - 7

5.2. Control de la Aplicación

Algunos de los scripts WMI ayudan a mantener el cumplimiento de las políticas de la organización en lo que respecta al uso de aplicaciones. Utilizando sólo la consola de administración. El administrador de sistemas puede saber fácilmente que software está instalado en los clientes y desinstalar cualquier aplicación no deseada.

1er Paso – Verificando las aplicaciones instaladas

El script **listar software instalado** puede utilizarse para obtener una lista de aplicaciones instaladas en el cliente con el instalador de Windows. Una vez se ejecute el script, el administrador de sistemas puede analizar los resultados en la consola de administración.

La imagen a continuación ofrece un ejemplo de los resultados para una estación de trabajo. En este ejemplo, la **Aplicación Genérica** es una aplicación no deseada que debería eliminarse.

Index	Caption	Description	Version	Install date
1.	Compatibility Pack for the 2007 Office system	Compatibility Pack for the 2007 Office system	12.0.6215.1000	20080614
2.	**Generic Application**	**Used as example**	1.6.0.50	20070917
3.	MSXML 4.0 SP2 (KB936181)	MSXML 4.0 SP2 (KB936181)	4.20.9848.0	20070913
4.	Microsoft .NET Framework 3.0 Service Pack 1	Microsoft .NET Framework 3.0 Service Pack 1	3.1.21022	20071214
5.	Apple Software Update	Apple Software Update	2.1.0.110	20080625
6.	Microsoft .NET Framework 2.0 Service Pack 1	Microsoft .NET Framework 2.0 Service Pack 1	2.1.21022	20071214
7.	Microsoft Office XP Professional with FrontPage	Microsoft Office XP Professional with FrontPage	10.0.6626.0	20070912
8.	QuickTime	QuickTime	7.4.0.91	20080206
9.	BitDefender Management Agent	BitDefender Management Agent	3.0.2	20080807
10.	Microsoft Virtual PC 2007	Microsoft Virtual PC 2007	6.0.156.0	20070914
11.	Software Update for Web Folders	Software Update for Web Folders	9.60.6715.0	20070912
12.	Adobe Photoshop CS2	Adobe Photoshop CS2	9.0	20070913
13.	MSXML 4.0 SP2 (KB927978)	MSXML 4.0 SP2 (KB927978)		
14.	MSXML 6.0 Parser (KB933579)	MSXML 6.0 Parser (KB933579)	6.10.1200.0	20070913
15.	MSXML 6.0 Parser	MSXML 6.0 Parser		
16.	Windows Presentation Foundation	Windows Presentation Foundation	3.0.6920.0	20071119
17.	Adobe Acrobat 7.0 Professional	Adobe Acrobat 7.0 Professional	7.1.0	20080516
18.	TortoiseSVN 1.4.8.12137 (32 bit)	TortoiseSVN 1.4.8.12137 (32 bit)	1.4.12137	20070913

Otros scripts de utilidad

Otros dos scripts pueden ofrecer información adicional sobre el software instalado en las estaciones de trabajo:
Enumerar menú de arranque recupera las aplicaciones que tienen accesos directos en el menú de Inicio.
Procesos en uso ofrece información sobre los procesos que se están ejecutando en ese momento en la estación de trabajo.

2º paso – Eliminando Aplicaciones Instaladas

Si una aplicación instalada en una estación de trabajo no cumple con las políticas de uso de aplicación, puede ser desinstalado fácilmente utilizando el script **Eliminar Software**. Este script hace uso del applet **Agregar o Quitar Programas** en el Panel de control para desinstalar aplicaciones instaladas en las estaciones de trabajo.

Aquí tiene algunos ejemplos de tipos de aplicaciones que pueden ser desinstaladas remotamente utilizando este script:
• Antivirus
• Programas de intercambio
• Chat
• Multimedia
• Juegos

El administrador de sistemas solo tiene que dar el nombre de la aplicación (como aparece en **Agregar o Quitar Programas** o en el script **Listar Software Instalado**) y ejecutar el script en la correspondiente estación de trabajo. La aplicación puede ser eliminada de la estación de trabajo sin la intervención de ningún usuario.

Desinstalar Software

En el ejemplo anterior, la **Aplicación Genérica** era una aplicación no deseada. Para desinstalarla, el administrador de sistemas debe dar el mismo nombre que se encuentra en el script del **Listar Software Instalado**.

Apéndice. Descripción de plantillas script WMI

Este apéndice ofrece una descripción detallada de las plantillas disponibles de script WMI.

Reinicio del equipo
Reinicia los equipos de trabajo

Apagado del equipo
Apaga las estaciones de trabajo

Procesos en uso
Ofrece información de los procesos que están actualmente ejecutándose en las estaciones de trabajo.

Recursos compartidos actuales
Ofrece información sobre las comparticiones existentes en las estaciones de trabajo.

Enumerar memoria
Muestra el tamaño de memoria física (RAM) instalada en las estaciones de trabajo

Enumerar archivo de paginación
Muestra información sobre la memoria virtual (el archivo de paginación) disponible en las estaciones de trabajo. Incluye:

- Localización y tamaño de la página de localización
- El tamaño inicial y máximo

Enumerar menú de arranque
Muestra información sobre los programas que se ejecutan en una estación de trabajo al iniciarse.

Espacio libre en disco
Muestra la lista de discos lógicos en las estaciones de trabajo y el espacio disponible en cada uno de ellos.

Consultar último SP instalado
Muestra la versión del Windows Service Pack instalado en las estaciones de trabajo.

Consultar información del Sistema
Muestra información útil sobre las estaciones de trabajo que incluye:

- Información del sistema operativo
- Nombre del sistema, modelo y fabricante
- Total de memoria RAM
- Procesador
- Versión BIOS

Detener proceso
Finaliza un proceso específico que esté siendo ejecutado en las estaciones de trabajo. El script

Procesos en uso
Puede usarse para obtener el listado de procesos en ejecución.

Listar información de la CPU
Muestra información sobre el procesador de las estaciones de trabajo que incluye:
- Nombre e ID del procesador
- Descripción
- Fabricante
- Velocidad del reloj

Listar usuarios existentes
Muestra los usuarios que están actualmente en sesiones de trabajo

Listar Información del Dominio y Grupo de Trabajo
Muestra información del dominio o grupo de estaciones de trabajo al que pertenece.

Listar Parches
Muestra información sobre los parches de Microsoft y Windows instalados en la estación de trabajo.

Listar software instalado
Muestra una lista de software instalado en las estaciones de trabajo con el instalador de Windows

Listar usuarios locales
Muestra información sobre las cuentas de usuarios locales en Windows configurados en las estaciones de trabajo

Mostrar información de discos lógicos
Muestra información sobre los discos lógicos (Disquetera, unidades de disco duro, Unidad de CD-ROM, etc.) en las estaciones de trabajo que incluye:
- Nombre (etiqueta)
- Descripción
- Espacio libre en disco
- Tamaño

Listar información de inicio de sesión
Muestra información referente a las sesiones abiertas en las estaciones de trabajo

Listar configuración de Placa Base
Muestra información de la placa base de las estaciones de trabajo que incluye:
- Nombre
- Fabricante
- Número de serie

Listar configuración del monitor

Muestra información sobre el monitor de las estaciones de trabajo, que incluye:

- Tipo de monitor
- Fabricante
- Dimensiones físicas

Listar valores de adaptadores de red

Ofrece información detallada de los adaptadores de red instalados en las estaciones de trabajo, que incluye:

- Tipo de adaptador
- Fabricante
- Dirección de red y MAC

Listar información de la administración de energía

Muestra información sobre la administración de energía de las estaciones de trabajo.

Listar Servicios

Muestra información sobre los servicios que se estén ejecutando en las estaciones de trabajo, que incluye:

- Nombre del Servicio y nombre mostrado
- Estado (inactivo / ejecutándose)
- Modo de inicio (auto / manual / desactivado)
- Descripción

Listar información de arranque

Ofrece información sobre el arranque de las estaciones de trabajo

Listar menú de arranque

Lista todos los atajos de programa del menú de inicio de las estaciones de trabajo. Las entradas son agrupadas por usuario.

Listar información de video

Ofrece información diversa sobre la visualización de video de las estaciones de trabajo, que incluye:

- Adaptador de video y tipo
- Memoria gráfica
- Resolución
- Nombre y versión del driver
- Ratio de refresco máximo y mínimo

Listar configuración WMI

Ofrece información sobre la configuración de WMI en las estaciones de trabajo.

Cerrar sesión del usuario

Cierra la sesión actual del usuario en las estaciones de trabajo.

Sistema operativo

Ofrece información útil sobre el sistema operativo ejecutado en las estaciones de trabajo, que incluye:

- Sistema operativo y versión
- Usuario registrado
- Número de serie
- Tiempo de instalación

Eliminar Software

Elimina una aplicación específica instalada en las estaciones de trabajo. El script puede usarse para eliminar cualquier aplicación que aparezca en el applet **Agregar y Quitar Programas** del Panel de Control.

Ejecutar Programa

Ejecuta una aplicación específica en las estaciones de trabajo. La aplicación puede ser localizada en la estación de trabajo deseada o en el equipo del administrador del sistema.