

PANDORAFMS
E N T E R P R I S E

Pandora FMS
Manual Administrador
Monitorización Sistemas Windows



Manual Administrador Monitorización Sistemas Windows

© Artica Soluciones Tecnológicas 2005-2012

Índice de contenido

1	Histórico de cambios.....	3
2	Introducción.....	4
3	Matriz de compatibilidad	5
4	Documentación a entregar por el Área que requiere la monitorización.....	6
5	Módulos del plugin.....	7
6	Definición de los módulos.....	8
6.1.	Módulos generales.....	8
6.1.1.	CPU Load.....	8
6.1.2.	Number processes.....	8
6.1.3.	Free Memory.....	9
6.1.4.	Disk discovery.....	9
6.1.5.	WMI Service	9
6.1.6.	SNMP Service	9
6.2.	Módulos de eventos.....	10
6.2.1.	Domain Auth. Fail.....	10
6.2.2.	Disk Structure Corrupted.....	10
6.2.3.	No domain controller.....	11
6.2.4.	Account blocked.....	11
6.2.5.	Account deleted.....	11
6.2.6.	Account disabled.....	12
6.2.7.	Password reset.....	12
6.2.8.	Password change.....	12
6.2.9.	Account enabled.....	13

1 HISTÓRICO DE CAMBIOS

Fecha	Autor	Cambio	Versión
17/03/12	Dario	Primera versión del plugin	v1r1

2 INTRODUCCIÓN

Este documento tiene como objetivo la descripción de la monitorización de cualquier máquina con sistema Operativo Windows.

Se han elegido una serie de módulos en base a nuestra experiencia en monitorización de sistemas y las necesidades de algunos de nuestros clientes.

Para la extracción de la información se utilizan:

- Capa de recolección, para los módulos de Pandora FMS susceptibles de ello, reduciendo así la carga de los sistemas a monitorizar.
- Módulos de tipo *module_exec* si es un comando.
- Módulos de tipo *module_plugin* si hablamos de un plugin de agente.

3 MATRIZ DE COMPATIBILIDAD

La matriz de compatibilidad para el plugin se muestra a continuación:

Sistemas donde se ha probado	<ul style="list-style-type: none"> • Windows 2003 Server • Windows 2008 Server • Windows XP
-------------------------------------	--

Sistemas donde debería funcionar	<ul style="list-style-type: none"> • Mismo sistema o superior
---	--

4 DOCUMENTACIÓN A ENTREGAR POR EL ÁREA QUE REQUIERE LA MONITORIZACIÓN.

La información que debe entregar el área que requiere la monitorización es la siguiente:

- El usuario que ejecute el agente de Pandora FMS debe tener los suficientes permisos para ejecutar los comandos y acceder a los ficheros necesarios sin problemas.
- Requisitos para que funcione correctamente esta monitorización son los siguientes:
 - Agente Pandora FMS instalado
- Información para los módulos:
 - Servicios a monitorizar
 - Discos a monitorizar

5 MÓDULOS DEL PLUGIN

- **CPU Load:** Este módulo devuelve el porcentaje de CPU en uso.
- **Number processes:** Módulo que devuelve el número de procesos del sistema.
- **Free Memory:** Módulo que devuelve el porcentaje de memoria libre del sistema.
- **Disk discovery:** Plugin que realiza un autdescubrimiento de discos y monitoriza su espacio ocupado.
- **WMI Service:** Módulo que comprueba si el servicio WMI está activo.
- **SNMP Service:** Módulo que comprueba si el servicio SNMP está activo.
- **Domain Auth. Fail:** Este módulo busca el evento que informa de un fallo en la autenticación del dominio.
- **Disk Structure Corrupted:** Este módulo busca el evento que informa de un fallo en la estructura del disco.
- **No domain controller:** Este módulo busca el evento que informa de que no se ha encontrado un controlador para el dominio.
- **Account blocked:** Este módulo busca el evento que informa que la cuenta está bloqueada.
- **Account deleted:** Este módulo busca el evento que informa que la cuenta ha sido borrada.
- **Account disabled:** Este módulo busca el evento que informa que la cuenta ha sido deshabilitada.
- **Password reset:** Este módulo busca el evento que informa que la contraseña ha sido reseteada.
- **Password change:** Este módulo busca el evento que informa que la contraseña ha sido cambiada.
- **Account enabled:** Este módulo busca el evento que informa que la cuenta ha sido habilitada.

6 DEFINICIÓN DE LOS MÓDULOS

A continuación se describen los diferentes módulos de monitorización, así como el código de cada uno de ellos.

6.1. Módulos generales

6.1.1. *CPU Load*

Este módulo devuelve el porcentaje de CPU en uso. La sintaxis para el módulo sería la siguiente:

```
module_begin
module_name CPU Load
module_type generic_data
module_wmiquery SELECT LoadPercentage FROM Win32_Processor
module_wmicolumn LoadPercentage
module_description CPU Load (%)
module_min_warning 80
module_max_warning 90
module_min_critical 91
module_max_critical 100
module_end
```

6.1.2. *Number processes*

Módulo que devuelve el número de procesos del sistema. Su sintáxis es la siguiente:

```
module_begin
module_name Number processes
module_type generic_data
module_exec tasklist | gawk "NR > 3 {print$0}" | wc -l
module_description Number of processes running
module_min_warning 175
module_max_warning 249
module_min_critical 250
module_max_critical 300
module_end
```


6.1.3. *Free Memory*

Módulo que devuelve el porcentaje de memoria libre del sistema. Su sintáxis es la siguiente:

```
module_begin
module_name Free Memory
module_type generic_data
module_freepcentmemory
module_description Free memory (%).
module_min_warning 21
module_max_warning 30
module_min_critical 0
module_max_critical 20
module_end
```

6.1.4. *Disk discovery*

Plugin que realiza un autdescubrimiento de discos y monitoriza su espacio ocupado. Su sintáxis es la siguiente:

```
module_plugin cscript.exe //B "%ProgramFiles%\Pandora_Agent\util\df.vbs"
```

6.1.5. *WMI Service*

Módulo que comprueba si el servicio WMI está activo. Su sintáxis es la siguiente:

```
module_begin
module_name WMI Service
module_type generic_proc
module_service winmgmt
module_description WMI Service enabled
module_end
```

6.1.6. *SNMP Service*

Módulo que comprueba si el servicio SNMP está activo. Su sintáxis es la siguiente:

```
module_begin
module_name SNMP Service
module_type generic_proc
module_service SNMP
module_description SNMP Service enabled
module_end
```

6.2. Módulos de eventos

6.2.1. *Domain Auth. Fail*

Este módulo busca el evento que informa de un fallo en la autenticación del dominio. La sintaxis para el módulo sería la siguiente:

```
module_begin
module_name Domain Auth Fail
module_type async_string
module_logevent
module_source System
module_eventcode 3210
module_description Domain Authentication Failure
module_end
```

6.2.2. *Disk Structure Corrupted*

Este módulo busca el evento que informa de un fallo en la estructura del disco. La sintaxis para el módulo sería la siguiente:

```
module_begin
module_name Disk Structure Corrupted
module_type async_string
module_logevent
module_source System
module_eventcode 55
module_application Ntfs
module_description Disk structure corrupted
module_end
```

6.2.3. *No domain controller*

Este módulo busca el evento que informa de que no se ha encontrado un controlador para el dominio. La sintaxis para el módulo sería la siguiente:

```
module_begin
module_name No domain controller
module_type async_string
module_logevent
module_source System
module_eventcode 5719
module_application NETLOGON
module_description Domain controller not found
module_end
```

6.2.4. *Account blocked*

Este módulo busca el evento que informa que la cuenta está bloqueada. La sintaxis para el módulo sería la siguiente:

```
module_begin
module_name Account blocked
module_type async_string
module_logevent
module_source Security
module_eventcode 4740
module_description Account blocked
module_end
```

6.2.5. *Account deleted*

Este módulo busca el evento que informa que la cuenta ha sido borrada. La sintaxis para el módulo sería la siguiente:

```
module_begin
module_name Account deleted
module_type async_string
module_logevent
module_source Security
module_eventcode 4726
module_description Account deleted
module_end
```

6.2.6. *Account disabled*

Este módulo busca el evento que informa que la cuenta ha sido deshabilitada. La sintaxis para el módulo sería la siguiente:

```
module_begin
module_name Account disabled
module_type async_string
module_logevent
module_source Security
module_eventcode 4725
module_description Account disabled
module_end
```

6.2.7. *Password reset*

Este módulo busca el evento que informa que la contraseña ha sido reseteada. La sintaxis para el módulo sería la siguiente:

```
module_begin
module_name Password reset
module_type async_string
module_logevent
module_source Security
module_eventcode 4724
module_description Password reset
module_end
```

6.2.8. *Password change*

Este módulo busca el evento que informa que la contraseña ha sido cambiada. La sintaxis para el módulo sería la siguiente:

```
module_begin
module_name Password change
module_type async_string
module_logevent
module_source Security
module_eventcode 4723
module_description Password change
module_end
```

6.2.9. *Account enabled*

Este módulo busca el evento que informa que la cuenta ha sido habilitada. La sintaxis para el módulo sería la siguiente:

```
module_begin
module_name Account enabled
module_type async_string
module_logevent
module_source Security
module_eventcode 4722
module_description Account enabled
module_end
```