

Инвентаризация



From:
 https://pandorafms.com/manual/!779/
 Permanent link:
 https://pandorafms.com/manual/!779/ru/documentation/04_using/04_inventory
 2025/01/22 19:13

Инвентаризация

Вернуться в оглавление Документации Pandora FMS

Инвентаризация

Введение

Enterprise версия Pandora FMS позволяет вести инвентаризацию устройств, контролируемых Pandora FMS. С помощью такой инвентаризации можно вести список процессоров, карт, оперативной памяти, патчей, программного обеспечения и т.д. серверов компании.

Инвентаризация не зависит от мониторинга и может быть получена локально (через программные агенты Pandora FMS) или удаленно:

- [©]Модель и скорость процессора (MS Windows®, GNU/Linux®).
- 🗁 Хранилище и файловые системы.
- 🛄 Версия прошивки (сетевое оборудование).
- 🕮 Конфигурация устройства (сетевое оборудование).
- 🕮 Серийные номера и лицензии (например: MS Office®, MS Windows®).
- Тустановленные на компьютере приложения (MS Windows®, Android Linux®, GNU/Linux®).
- 🚧 Сетевые карты и их МАС-адреса, связанные с IP-адресами.
- Стати в стания в стания в стания и мак объем (MS Windows®, GNU/Linux®).
- 💞 Рут установлены.
- 🧐 Запуск сервисов.
- Читройства хранения (MS Windows®, GNU/Linux®).
- 🖾 Системные пользователи.

Сбор данных для инвентаризации

Сбор данных для инвентаризации систем осуществляется двумя способами:

Удаленно, с помощью модулей инвентаризации, через *скрипты* интегрированные в Pandora FMS, которые выполняют *queries* WMI, или *скрипты*, выполняемые через SSH с помощью Expect или аналогично.

На местном уровне, с помощью программного агента Pandora FMS, через плагины в агенте.

Модули инвентаризации

Модули инвентаризации - это удаленные модули, которые выполняют команду на удаленной машине. Эти модули работают аналогично *плагину*. Те же модули могут быть определены как «локальные», если они получают данные через агента.

В параметрах пользователя и пароля можно использовать следующие макросы: _agentcustomfield_n_ (Пользовательское поле номера агента).

Удаленная инвентаризация

Создание удаленных модулей

Создание администратором модуля удаленной инвентаризации не является обычным делом; они уже поставляются с предустановленным Pandora FMS Enterprise. Однако Pandora FMS позволяет создавать собственные модули инвентаризации или изменять существующие с помощью редактора модулей инвентаризации.

Чтобы создать удаленный модуль, перейдите в раздел Configuration → Inventory Modules, где перечислены все созданные модули инвентаризации.

	RAFMS ←	Pandora FMS the Flexible Monitoring System						
Operation	Management	Configuration / Inventory modules Inventory modules						
A Discovery	~							
Resources	~		Name	Descriptic				
Profiles	~		CPU	CPU				
Configuration	^		CPU	CPU				
Templates	~		RAM	Memory m				
Inventory module	S		RAM	Memory m				
Manage agent aut	oconfiguration		Video	Video card:				
Software agents re	epository		Video	Video carde				
Manage policies			NIC	Network In				
Collections			NIC	Network In				

Чтобы создать новый модуль, нажмите на Create.

Configuration / Inventory modules Module management

Name	Description
OS	Interpreter
Linux	~
	Left blank for the LOCAL inventory modules
Format	Block mode
separate fields with ;	
Script mode	
Script mode Use inline code	
Script path	
	Go back 🕥 🛛 Create 🥑

OS: Выберите целевую операционную систему для модуля.

Interpreter: Оставьте пустым, если это локальный модуль. Поле, в которое помещается командный интерпретатор, используемый в модуле. Это может быть Shell Script, Perl или другой допустимый интерпретатор для сервера инвентаризации, работающего в системе Linux.

Block mode: Отображает и обнаруживает изменения в конфигурации.

Format: Введите поля, разделенные ; , которые будут возвращены модулем.

Code: Оставьте пустым, если это локальный модуль. Код модуля; обычно это код Perl или Shell Script. Если бы это был двоичный код, то ему потребовалась бы другая процедура загрузки, вводимая вспомогательными скриптами.

Очень важно правильно выбрать операционную систему, так как при добавлении дополнительных модулей инвентаризации в агенте появятся только те модули, операционная система которых соответствует операционной системе модуля и операционной системе агента.

۲

После создания модуля нажмите кнопку Create:

MODULE MANAGEMENT » INVENTORY MODULES

Name	Software
Description	Installed software packages
O5	Windows
Interpreter	/usr/bin/perl (i)
Block mode	
Format	Name;Version
Script mode (Use script 🔿 Use inline code 🧿
	<pre>#!/usr/bin/perl ##!/usr/bin/perl ####################################</pre>
Code (i)	<pre># as published by the Free Software Foundation; version 2. # # This program is distributed in the hope that it will be useful, # but WITHOUT ANY WARRANTY; without even the implied warranty of # MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the # GNU General Public License for more details. # You should have received a copy of the GNU General Public License # along with this program; if not, write to the Free Software # Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA. ####################################</pre>
	Create ()

редактирование удаленных модуля

Чтобы отредактировать удаленный модуль, перейдите в Configuration → Inventory Modules,

где перечислены все созданные модули инвентаризации. Нажмите на в названии модуль, который вы хотите отредактировать, или на иконку ключа в колонке Action.

MODULE MANAGEMENT » INVENTORY MODULES							
Total items: 37				0 1			
Name	Description	OS	Interpreter	Action 🗌			
CPU	CPU	Δ	Remote/Local	₽ 🗖 🗆			

Снова появится страница создания модуля.

MODULE MANAGEMENT » INVENTORY MODULES

Name	CPU
Description	CPU
OS	Linux
Interpreter	/usr/bin/perl ()
Block mode	
Format	Model;Company;Speed
	#!/usr/bin/perl ####################################
Code 🕕	# Copyright (c) 2008 Ramon Novoa, rnovoa@artica.es
	# (c) 2008 Artica Soluciones Tecnologicas S.L
	#
	# This program is free software; you can redistribute it and/or
	# modify it under the terms of the GNU General Public License
	# as published by the Free Software Foundation; version 2.
	# # This program is distributed in the bane that it will be useful
	# hut WITHOUT ANY WARRANTY: without even the implied warranty of
	# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
	# GNU General Public License for more details.
	# You should have received a copy of the GNU General Public License
	# along with this program; if not, write to the Free Software
	Update >

Pandora FMS v7.0NG.759 - OUM 759 - MR 51 Page generated on 2022-01-07 09:32:16

Измените нужные поля и нажмите на кнопку. Update.

Уничтожение удаленных модулей

Чтобы удалить удаленный модуль, перейдите в раздел Configuration \rightarrow Inventory Modules,

где перечислены все созданные модули инвентаризации. Нажмите на значок корзины в столбце Action модуля, который необходимо удалить.

MODULE MAN	MODULE MANAGEMENT » INVENTORY MODULES								
Total items: 37				0 1					
Name	Description	OS	Interpreter	Action 🗌					
CPU	CPU	Δ	Remote/Local	۵ 🖉 🏕					

Кроме того, каждый из них имеет флажок, который позволяет выбирать их пакетно, а не удалять по одному.

Назначение удаленных модулей

Назначение модулей инвентаризации осуществляется в самом агенте, на вкладке администрирования агента.

Вы должны нажать на вкладку Inventory.

Resources / Manage agents / Setup	Inventory	☆ ⊚
Agent name 275760bebf9a9c39a6361fcea ID 40 Q 👼 🖸	Interval 5 minutes View age	ent QR code
Alias KEPLER	os Windows	
IP Address 192.168.56.1 Unique IP	Server The server	
192.168.56.1 Delete selected items	Description Cust	:om ID:
Primary group Workstations		

Откроется страница, на которой можно добавить модули инвентаризации.

Resources / Manage agen KEPLER	ts / Inventory	p	●.	Ψ	•	*	¥	∎O ☆▲	.	*	쭛.	٥	*	0
Module	CPU ·			Inter	val			11	iour	Ŧ				
Target	192.168.56.1			Use c	ustom fiel	ds								
Username	PandoraFMS			Passv	Password		•••••							
														Add >
P. Name		Description				Target	t	I.	nterval			Act	tions	
Software	Installed software package	ES					5	i minutes			ā /	• 0		

- Module: Выберите модуль инвентаризации, который необходимо добавить. Будут отображаться только те модули, операционная система которых совпадает с операционной системой агента.
- Target: IP-адрес или имя сервера, с которого вы хотите произвести инвентаризацию.
- Interval: Выберите интервал времени, через который запускается модуль инвентаризации.
- Username: Пользователь, который будет использоваться для запуска модуля инвентаризации.
- Password: Пароль пользователя, который будет использоваться для запуска модуля инвентаризации.

Начиная с версии v7.0NG.724, можно определять поля вместо обычных полей пользователя и пароля. Для этого необходимо активировать следующий флажок:



После этого появится элемент управления для добавления новых полей (Add field):

Field name	It's a password	Add field	0	
		L		

В этом элементе управления введите нужное имя перед его добавлением. Если вы укажете, что поле должно содержать пароль, значение будет храниться в базе данных в сокрытом виде.

После создания полей мы можем присвоить им значение и, наконец, добавить модуль. Эти поля должны применяться в порядке создания при выполнении *скрипта* удаленной инвентаризации.

Module	CPU 💌	Interval	1hour 🔻
Target	192.168.56.1	Use custom fields	
Username	PandoraFMS	1	
Password	•••••	_	
Enable password	•••••	1	
Field name		's a password Add field 💿	

После заполнения формы нажмите кнопку Add. Модуль будет добавлен в модули инвентаризации.

	SUCCESS Inventory mode	ule added successfully				×
Mod	lule	Select inventory mod 💌		Interval	1 hour 💌	
Targ	et	192.168.56.1		Use custom fields		
User	mame			Password		
						Add >
P	Name	Descrip	ption	Target	Interval	Actions
	CPU	CPU		192.168.56.1	1 hours	亩 ≁ Ο
	Software	Installed software packages			5 minutes	± ○
		Pandora FMS Page genera	v7.0NG.759 - OUM 759 - MR ated on 2022-01-07 10:33:44	51 +		

Редактирование назначенного модуля удаленной инвентаризации

Модули инвентаризации можно редактировать; это редактирование осуществляется на той же странице, где они были созданы.

Чтобы отредактировать модуль инвентаризации, нажмите на название модуля или на значок ключа, показанный на рисунке.

P.	Name	Description	Target	Interval			Actions
	CPU	CPU	192.168.56.1	1 hours	ŵ	Þ	0
	Software	Installed software packages		5 minutes	ŵ	p	0

Удаление назначенного удаленного модуля инвентаризации

Можно удалять модули инвентаризации; удаление производится на той же странице, где они были созданы.

R	Name	Description	Target	Interval		Actions
	CPU	CPU	192.168.56.1	1 hours	亩	۶O
	Software	Installed software packages		5 minutes	ŵ	FO

Чтобы удалить модуль инвентаризации, нажмите на значок корзины в колонке Action модуля.

Полный пример процесса создания удаленного модуля инвентаризации

Предположим, вам нужно получить список физических адресов адаптера с сервера, в данном случае сервера Unix. Эту информацию обычно получают с помощью команды arp - a - n, которая при запуске на сервере будет выглядеть примерно так:

```
artica@galaga:~$ arp -a -n
? (192.168.70.74) at 08:00:27:39:BF:6F [ether] on eth2
? (192.168.70.162) at B4:74:9F:94:98:84 [ether] on eth2
? (192.168.50.30) at 08:00:27:10:D1:1A [ether] on eth0
? (192.168.70.90) at 98:0C:82:54:2F:DE [ether] on eth2
? (192.168.50.2) at 08:00:27:EA:B2:FF [ether] on eth0
? (192.168.70.135) at C8:60:00:4B:96:67 [ether] on eth2
? (192.168.60.182) at FE:26:C5:91:B1:DA [ether] on tap0
```

В данном примере мы ищем IP-адрес, MAC-адрес и имя адаптера.

В Shellscript это можно сделать следующим образом, используя «» для разделения полей:

arp -a -n | sort | grep -v incomplete | awk '{ print \$2,\$4,\$7 }'

Это то, что необходимо для «импорта» этой информации в сервер удаленной инвентаризации Pandora FMS. Для этого возьмите за основу слегка модифицированный модуль удаленной инвентаризации «CPU». Этот *скрипт* подключается через SSH к целевому

серверу и выполняет команду. Вывод команды должен возвращать каждое поле, разделенное символом ; .

На этом этапе вам необходимо иметь навыки программирования, чтобы разработать или изменить *скрипты*. *Скрипты* удаленной инвентаризациии, хотя и не сложные, требуют определенных знаний Perl, Shellscript или другого интерпретируемого языка; они также могут быть выполнены на Java, C++, и вызывать их выполнение из модуля, при условии, что он возвращает значения каждого определенного поля, разделенные ; и переходом строки для каждой единицы данных.

#!/usr/bin/perl # pandora linux arptable.pl # Copyright (c) 2012 Sancho Lerena <slerena@artica.es> (c) 2012 Artica Soluciones Tecnologicas S.L # # # This program is free software; you can redistribute it and/or # modify it under the terms of the GNU General Public License # as published by the Free Software Foundation; version 2. # # This program is distributed in the hope that it will be useful, # but WITHOUT ANY WARRANTY; without even the implied warranty of # MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the # GNU General Public License for more details. # You should have received a copy of the GNU General Public License # along with this program; if not, write to the Free Software # Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.

```
use strict;
use warnings;
# Check for ssh
my $ssh_client = "ssh";
if (system("$ssh_client -v> /dev/null 2>&1")>> 8 != 255) {
    print "[error] $ssh_client not found.\n";
    exit 1;
}
if ($#ARGV <1) {
    print "Usage: $0 <target ip> <username>\n";
    exit 1;
}
my $target_ip = $ARGV[0];
my $username = $ARGV[1];
```

```
# Retrieve ARP table
my ($ip, $mac, $iface);
my $command = '/usr/sbin/arp -a -n | sort | grep -v incomplete | awk \'{ print
\$2,\$4,\$7 }\'';
my @info = `$ssh_client $username\@$target_ip "$command" 2> /dev/null`;
foreach my $line (@info) {
    if ($line =~ /^(.+)\s(.+)/) {
        $ip = $1;
        $mac = $2;
        $iface = $3;
        print "$ip;$mac;$iface\n";
    }
}
exit 0;
```

Чтобы SSH-соединение работало автоматически, необходимо скопировать открытый ключ пользователя root с сервера Pandora FMS на целевой сервер. Если целевое устройство имеет следующий IP-адрес, например, 192.168.50.10, выполните следующие действия:

1. Создайте ключ на сервере Pandora FMS как корень. Заполните необходимые поля.

ssh-keygen

2. Используйте команду ssh-copy-id для копирования открытого ключа на целевой сервер (192.168.50.10) с целевым пользователем (в данном примере пользователем с именем artica):

ssh-copy-id -i /root/.ssh/id_rsa.pub artica@192.168.50.10

Вы должны ввести пароль пользователя artica один раз на 192.168.50.10, чтобы установить открытый ключ на целевом сервере.

3. Попробуйте подключиться; подключение произойдет без запроса пароля:

ssh artica@192.168.50.10

4. Если вы дошли до этого, тот же процесс будет выполняться и модулем инвентаризации, поэтому попробуйте запустить его из командной строки, сохранив предыдущий *скрипт* на диск (файл temporal.pl, т.е.) и запустить его с IP-адресом и пользователем как параметр:

perl temporal.pl 192.168.50.10 artica
(192.168.50.1);00:0f:ea:27:ba:f0;eth0
(192.168.50.3);08:00:27:98:f8:48;eth0

Обратите внимание, что скрипт удаленно вызывает /usr/sbin/arp. Команда должна

находиться в этом пути; если нет, переместите скрипт в другое место. Вы также можете заметить, что мы вызываем наш *скрипт* с помощью команды perl, которая обычно находится в /usr/bin/perl. Это то, что вы должны настроить при определении модуля, как показано ниже:

Description ARP Inventory OS Linux Interpreter /usr/bin/perl Block mode	Name	ARP
OS Linux Interpreter Assr/bin/perl Block mode	Description	ARP Inventory
Interpreter Just/bin/perl Block mode - Format ipmacjiface Code #Just/bin/perl #Justr/bin/perl #Justr/bin/perl #copyright (c) 2012 Sancho Lerena <slerena@artica.es> # (c) 2012 Artica Soluciones Tecnologicas SL # This program is free software you can redistribute it and/or # modify it under the terms of the GNU General Public License # as published by the Free Software Foundation; version 2. # This program is distributed in the hope that it will be useful. # but WITH/OUT ANY WARRANTY; without even the inplied warranty of # CROU General Public License for more details. # You should have received a copy of the GNU General Public License # along with this program; if not, write to the Free Software # Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA. # Event and the missing; # Check for ssh my \$ssh_client = "ssh";</slerena@artica.es>	OS	Linux 💌
Block mode ippmaciface Format Implement Implem	Interpreter	/usr/bin/perl (i)
Format ippmacjiface code #!/dsr/bin/perl #= pandora_linux_arptable.pl #= copyright (c) 2012 Sancho Lerena <slerena@artica.es> # (c) 2012 Artica Soluciones Tecnologicas SL # This program is free software; you can redistribute it and/or # ondify it under the terms of the GNU General Public License # as published by the Free Software Foundation; version 2. # # This program is distributed in the hope that it will be useful, # but WITHOUT ANY WARRANTY; without even the implied warranty of # MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the # GNU General Public License # Jou should have received a copy of the GNU General Public License # Jou should have received a copy of the GNU General Public License # Jou should have received a copy of the GNU General Public License # Jou should have received a copy of the GNU General Public License # Jou should have received a copy of the GNU General Public License # Jou should have received a copy of the GNU General Public License # Jou should have received a copy of the GNU General Public License # Jou should have received a copy of the GNU General Public License # Jou should have received a copy of the GNU General Public License # Sounder Shou</slerena@artica.es>	Block mode	
Code #!/usr/bin/perl ####################################	Format	ip;mac;iface
Create 🗷 🔨	Code (<pre>#/usr/bin/perl ####################################</pre>

Применяя его к агенту, убедитесь, что операционная система совпадает. Если у вас разные операционные системы, вы должны создать отдельный модуль для каждой из них, потому

что один и тот же код не будет работать.

Module	ARP	Interval	1 hour 🔻 💉
Target	192.168.70.147	Use custom fields	
Username		Password	

После выполнения этого модуля из консоли можно получить вид, подобный следующему:

Group	All	▼ Module	ARP	• Search Q
Agent	All) (i) Search		
Date	Last 💌	Order by agent		
400			• 0	Export this list to CSV ,a,
Agent	ip	mac	iface	Timestamp
ARP agent	(192.168.26.254) (192.168.26.2) (192.168.70.105) (192.168.70.156)	00:50:56:f3:e2 00:50:56:f0:14 98:54:1b:fb:b9 30:3a:64:a0:d2	2:7d ens38 4:58 ens38 9:58 ens33 7:c8 ens33	
	(192,168,70,198)	d0:67:e5:01:16	f:d3 ens33	

Локальная инвентаризация с помощью программных агентов

Mediante los C помощью программных агентов можно получить данные инвентаризации машины. Достаточно применить соответствующие модули инвентаризации в конфигурации программного агента.



Как и в случае с удаленными модулями, эти модули также необходимо добавить в качестве инвентарных модулей в Configuration → Inventory modules.

Создание локальных модулей

Чтобы создать локальный модуль, перейдите в раздел Configuration → Inventory modules, где перечислены все созданные модули инвентаризации. Здесь должны быть созданы все модули, определенные в конфигурации агента; операционная система, назначенная агенту в консоли, также должна совпадать с операционной системой созданного модуля.

MODULE MANAGEMENT » INVENTORY MODULES

Total items: 38				0 1
Name	Description	os	Interpreter	Action
CPU	CPU	۵	Remote/Local	ا ا ا ا ا ا ا
CPU	CPU		Remote/Local	# 🖻 🗆
RAM	Memory modules	۵	Local module	ا 🛣 🖉
RAM	Memory modules		Remote/Local	ا 🛣 🖉
Video	Video cards	Δ	Local module	۵ 🖈 🖈
Video	Video cards		Remote/Local	ا 🛣 🖉
NIC	Network Interface Cards	Δ	Local module	۵ 🖈 🖈
NIC	Network Interface Cards		Remote/Local	ا 🛣 🖉
HD	Hard drives	Δ	Local module	۵ 🛣 🖉
HD	Hard drives		Remote/Local	を 亩 🗆

Чтобы создать новый модуль, нажмите на Create.

MODULE MANAGEMENT » INVENTORY MODULES

Name		
Description		
os	Linux	
Interpreter	\bigcirc	
Block mode		
Format		
Code (i)		
	Create 🕚	
	Pandora FMS v7.0NG.759 - OUM 759 - MR 51	

Процедура такая же, как и для случая с удаленным модулем, за исключением заполнения полей Interpreter и Code. В данном примере для поля OS можно задать собственные операционные системы.

После заполнения полей нажмите кнопку Создать, чтобы сохранить. В списке модулей инвентаризации вы увидите что-то вроде этого изображения:

Software Remote	Get software from Remote MS Windows®		Remote/Local	۵ 🛣 🖉	
ARP	ARP Inventory	Δ	Remote/Local	# 🖮 🗆	
CPU	CPU	Ø	Local module	۵ 🛣 🖌	
Total items: 39				0 1	
			Create	> Delete 🍵	<u> </u>
	Pandora FMS v7.0NG.759 - OUM 759 - MF	151			
	Page generated on 2022-01-09 09:20:1	2			

Pour modifier le module d'inventaire nouvellement créé (ainsi que tous les autres), cliquez soit sur son nom, soit sur l'icône de la clé à molette.

Name	CPU	
Description	CPU	
OS	Ubuntu 💌	
Interpreter	0	
Block mode		
Format 🕕	Model;Company;Speed	
Code		
		/

Измените необходимые значения и нажмите кнопку Обновить, чтобы сохранить изменения.

Конфигурация локальной инвентаризации для программных агентов

Чтобы адаптировать конфигурацию программного агента к новой версии, необходимо:

1. Разверните коллекцию скриптов (загрузите из библиотеки Pandora FMS).

Начиная с версии 7, эти плагины по умолчанию поставляются вместе с установкой агента, хотя они закомментированы в конфигурационном файле.

2. Настройте запланированное выполнение *скриптов* локальной инвентаризации в файле pandora_agent.conf, добавив в конце следующую информацию:

Начиная с версии 7 и далее, нет необходимости в добавлении; просто откомментируйте существующие

плагины в конфигурационном файле Агента. Более подробную информацию можно найти в видеоуроке «Inventory modules in Windows» (повествование ведется на английском языке).

Пример для MS Windows®:

#module begin #module plugin cscript.exe //B //t:20 "%PROGRAMFILES%\Pandora Agent\util\cpuinfo.vbs" #module_crontab * 12-15 * * 1 #module_end #module begin #module plugin cscript.exe //B //t:20 "%PROGRAMFILES%\Pandora_Agent\util\moboinfo.vbs" #module crontab * 12-15 * * 1 #module_end #module begin #module_plugin cscript.exe //B //t:20 "%PROGRAMFILES%\Pandora Agent\util\diskdrives.vbs" #module crontab * 12-15 * * 1 #module end #module begin #module_plugin cscript.exe //B //t:20 "%PROGRAMFILES%\Pandora Agent\util\cdromdrives.vbs" #module crontab * 12-15 * * 1 #module end #module begin #module_plugin cscript.exe //B //t:20 "%PROGRAMFILES%\Pandora Agent\util\videocardinfo.vbs" #module_crontab * 12-15 * * 1 #module end #module begin #module plugin cscript.exe //B //t:20 "%PROGRAMFILES%\Pandora Agent\util\ifaces.vbs" #module crontab * 12-15 * * 1 #module_end #module begin #module plugin cscript.exe //B //t:20 "%PROGRAMFILES%\Pandora_Agent\util\monitors.vbs" #module crontab * 12-15 * * 1 #module_end

#module begin #module plugin cscript.exe //B //t:20 "%PROGRAMFILES%\Pandora Agent\util\printers.vbs" #module crontab * 12-15 * * 1 #module end #module begin #module_plugin cscript.exe //B //t:20 "%PROGRAMFILES%\Pandora Agent\util\raminfo.vbs" #module crontab * 12-15 * * 1 #module end #module begin #module_plugin cscript.exe //B //t:20 "%PROGRAMFILES%\Pandora Agent\util\software installed.vbs" #module crontab * 12-15 * * 1 #module end #module begin #module plugin cscript.exe //B //t:20 "%PROGRAMFILES%\Pandora Agent\util\userslogged.vbs" #module_crontab * 12-15 * * 1 #module end #module begin #module plugin cscript.exe //B //t:20 "%PROGRAMFILES%\Pandora_Agent\util\productkey.vbs" #module crontab * 12-15 * * 1 #module end #module begin #module plugin cscript.exe //B //t:20 "%PROGRAMFILES%\Pandora Agent\util\productID.vbs" #module crontab * 12-15 * * 1 #module_end

Модуль инвентаризации в системах Unix с помощью программного агента

Модуль программного агента Unix локально использует *плагин* для сбора информации о различных аспектах машины, как программных, так и аппаратных.

Синтаксис модуля следующий:

```
module_plugin inventory 1 cpu ram video nic hd cdrom software init_services
filesystem users route
```

Модуль состоит из строки со следующими параметрами:

• Активация модуля:

"module_plugin inventory" 1 cpu ram video nic hd cdrom software init_services
filesystem users route

• Поле, в котором устанавливается, с какой периодичностью (в днях) будет выполняться модуль. Если ноль (0), то инвентарь возвращается при каждом выполнении Агента.

module_plugin inventory "1" cpu ram video nic hd cdrom software init_services
filesystem users route

• Поле, в котором задаются объекты инвентаризации, подлежащие сбору.

module_plugin inventory 1 "cpu ram video nic hd cdrom software init_services
filesystem users route"

Как и в агенте для MS Windows®, можно собирать следующие объекты:

- СРU: Собирает информацию о центральных процессорах.
- ram: Собирает информацию о модулях оперативной памяти.
- video: Собирает информацию о видеокартах.
- nic: Собирает информацию о сетевых картах, Network Interface Controlers.
- hd: Собирает информацию о жестких дисках.
- cdrom: Собирает информацию об устройствах чтения оптических дисков.
- patches: Собирает информацию об установленных программных патчах.
- software: Собирает информацию об установленном программном обеспечении.
- init_services: Собирает информацию о процессах авто инициирования.
- filesystem: Собирает информацию о сегментации системы.
- users: Собирает информацию о пользователях.
- Route: Собирает информацию о таблице путей системы.

Плагин, который собирает инвентарь, находится в каталоге /etc/pandora/plugins.

Он также может быть задан просто для сбора всей доступной информации. В данном примере он ежедневно собирает всю информацию об инвентаризации:

Plugin for inventory on the agent (Only Enterprise)
module_plugin inventory 1

Чтобы активировать модуль инвентаризации, просто скопируйте описанный выше код в файл pandora_agent.conf программного агента, а затем перезапустите службу. Эта активация может быть из удаленной конфигурации агента (ьолее подробную информацию можно найти в видеоуроке «Inventory modules in Windows» (повествование ведется на английском языке) или выполнена локально:

agents / KEPLER	0	
Add module		
Group	General group Module None	Add 💿
Delete remote o	confagent files 📷 (i)	
# (c) 2006- # Version 7	2021 Artica Soluciones Tecnologicas 7.0NG.759	
# This prog published t the hope th	ram is Free Software, you can redistribute it and/or modify it # under the terms of the GNU General Public L by the # Free Software Foundation; either version 2 of the Licence or any later # version. This program is dist hat it will be useful,# but WITHOUT ANY WARRANTY, without ever the implied warranty of # MERCHANTA	icence as ributed in ABILITY or
FITNESS F	DR A PARTICULAR PURPOSE	
		Update 🔿
	Pandora FMS v7.0NG.759 - OUM 759 - MR 51	
	Page generated on 2022-01-09 10:36:44	

	BOKS BLULIV	MODVDOM
пазпачение	локальных	модулеи

Нет необходимости активировать модули в агентах, определенных в консоли. Если модули были созданы в Configuration → Inventory modules, операционная система соответствует, а выполнение определено в конфигурационном файле программного агента *собранные данные появятся напрямую* в разделе View → Inventory агента в консоли.

EPLER) (()		: 🖬 🖣		≜	*
Module All Tote	Now		- Search		Search ¥	
	CPU	- (January 9, 202)	2, 7:08 am)			
Name		Speed	Description			
Intel(R) Core(TM) i5-2400 CPU @ 3.10GH	z	3101 MH	Iz Intel64 Fami	ly 6 Model 42 Step	pping 7	
	NIC	- (January 9, 2022	2, 7:08 am)			
Caption			MACAddress	I	PAddress	
Intel(R) 82579LM Gigabit Network Conne	ction		44:37:E6:AC:4F:E	A 1	92.168.1.47	
	RAM	l - (January 9, 202	2, 7:08 am)			
Slot	Size		Spe	ed		
A1_DIMM0	20481	ИВ	133	33 MHz		
A1_DIMM1	20481	ИВ	133	33 MHz		
A1_DIMM2	20481	ИВ	133	33 MHz		
A1_DIMM3	20481	ИВ	133	33 MHz		

Page generated on 2022-01-09 12:15:51

Создание локальных модулей инвентаризации с помощью Software Agent

В дополнение к системам инвентаризации, предварительно настроенным в Агенте, вы можете легко создавать модули инвентаризации для систем Unix® и Windows®.

В основном вам нужно создать *скрипт*, который генерирует XML со следующей структурой:

```
<inventory>
<inventory_module>
<name>INVENTORY_MODULE_NAME</name>
<type>generic_data_string</type>
<datalist>
        <data>DATA1;DATA2;DATA3....</data>
</datalist>
</inventory_module>
</inventory>
```

INVENTORY_MODULE_NAME: Вы должны поместить то же имя модуля, которое вы

зарегистрировали в модулях инвентаризации в консоли Pandora FMS.

DATA1;DATA2... : Это данные, которые необходимо извлечь и которые были определены в модуле инвентаризации.

Предположим, вы хотите получить ARP-таблицу, IP-адрес с его интерфейсами (см. предыдущий пример с удаленными модулями инвентаризации). Используйте команду arp - а и очистите запись, чтобы получить нужные данные.

Теперь для разработки в MS Windows® сделайте небольшой *скрипт* C:\tmpwindows_arp_inventory.bat со следующим определением:

@echo off

```
echo ^<inventory^>
echo ^<inventory_module^>
echo ^<name^>ARP^</name^>
echo ^<type^>generic_data_string^</type^>
echo ^<datalist^>
arp -a | sort | grep "[0-9]" | grep -v ":" | gawk "{ print \"^<data^>\"
$1\";\"$2\";\"$3 \"^</data^>\" }"
echo ^</datalist^>
echo ^</datalist^>
echo ^</inventory_module^>
echo ^</inventory/>
```

Теперь вам нужно изменить pandora_agent.conf, и добавить следующую строку:

module_plugin cmd.exe /C C:\tmp\windows_arp_inventory.bat

Этот скрипт будет запускаться каждые 5 минут (по умолчанию - это интервал Агента). Если вы хотите, чтобы он запускался каждые X времени, вам придется реализовать эту логику в самом *скрипте* или использовать запланированный мониторинг

Помните: чтобы локальный script мог хранить информацию об инвентаризации, в консоли должен быть определен модуль инвентаризации, в котором указывается операционная система, имя модуля и данные для хранения, разделенные ; . Помните, что перед перезапуском агента Pandora FMS, чтобы загрузить внесенные изменения, создайте модуль инвентаризации в Pandora FMS:

MODULE MANAGEMENT » INVENTORY MODULES

Name	ARP
Description	ARP Inventory
OS	Windows
Interpreter	
Block mode	
Format (j)	ip;mac;iface

Обратите внимание, что, будучи локальным модулем, поля Interpreter и Code не нужны, хотя поле Operating System (OS) важно.

Полученные результаты совпадают с результатами, полученными для эквивалентного удаленного модуля в GNU Linux:

Group	All		*	Module	AR	P	•	Search Q
Agent	All	۹	()	Search				
Date	Last	•		Order by agent				
APP					•0		Export this li	st to CSV ,a,
Agent		ip		mac	0.	iface	Time	stamp
ARP agent		(192.168.26.254) (192.168.26.2) (192.168.70.105) (192.168.70.156) (192.168.70.198) (192.168.70.1) (192.168.70.1)		00:50:56:f3:e2 00:50:56:f0:14 98:54:1b:fb:b9 30:3a:64:a0:d d0:67:e5:01:11 c0:ea:e4:6e:98 0e:9f:75:49:5f	2:7d 4:58 9:b8 7:c8 f:d3 9:22 :02	ens38 ens38 ens33 ens33 ens33 ens33 ens33		
Total: 7		,,						

В онлайн-библиотеке модулей Pandora FMS имеется множество других модулей инвентаризации, как удаленных, так и локальных. Вы также можете легко разрабатывать свои собственные модули, как вы уже видели в этой главе.

Визуализация данных инвентаризации



31/42

32/42

Данные инвентаризации, собранные из системы, локально или удаленно, можно просмотреть из самого агента или из меню Инвентаря консоли.

Просмотр данных инвентаризации в меню Инвентаря

В разделе Monitoring → Inventory можно просмотреть данные инвентаризации всех агентов, выполнить поиск и экспортировать данные в CSV-файл.

Monitoring	RY					
Group	All		•	Module	All	
Agent	All		•	Search		Search Q
Date	Last	•		Order by agent		

Ниже перечислены поля, которые можно использовать для поиска.

- Group: Выберите группу агентов для фильтрации. Пользователь сможет увидеть группы, к которым он будет принадлежать, только если этот пользователь не принадлежит к группе BCE (ALL).
- Module: Выберите модуль инвентаризации, по которому вы хотите отфильтровать данные.
- Agent: Введите имя агента, по которому вы хотите отфильтровать.
- Search: Напишите текст для поиска по всем полям инвентаря.

С помощью поиска можно просмотреть модули всех агентов, у которых есть инвентарь, выбрав в параметрах поиска все и нажав на Search.

Agent		Model			Size Times	tamp	
RAM			(202	2-0	1-09 17:16:33)		
KEPLER	Intel(R)	Core(TM) i5-2400 CPU @ 3.10GHz	3101 MHz		Intel64 Family 6 Model 42 St	epping 7	2022-01-09 12:08:11
Agent	Name		Speed		Description		Timestamp
CPU			(202	2-0:	1-09 17:16:33)		
euclides		DO-Premium-AMD		٨d	vanced Micro Devices [AMD]	2GHz	2022-01-09 15:32:47
		Intel(R) Xeon(R) CPU E3-1230 v6 @ 3.5	0GHz	Inte	el Corp.	3504MHz	2022-01-09 17:54:33
		Intel(R) Xeon(R) CPU E3-1230 v6 @ 3.5	0GHz	Inte	el Corp.	3504MHz	2022-01-09 17:54:33
prueba_k	еер	Intel(R) Xeon(R) CPU E3-1230 v6 @ 3.5	0GHz	Inte	el Corp.	3504MHz	2022-01-09 17:54:33
		Intel(R) Xeon(R) CPU E3-1230 v6 @ 3.5	0GHz	Inte	el Corp.	3504MHz	2022-01-09 17:54:32
		Intel(R) Xeon(R) CPU E3-1230 v6 @ 3.5	.50GHz I		el Corp.	3504MHz	2022-01-09 17:54:32
munchkin	_agent	Intel(R) Xeon(R) CPU E3-1230 v6 @ 3.5	.50GHz I		el Corp.	3504MHz	2022-01-09 17:54:32
Agent		Model		Cor	mpany	Speed	Timestamp
CPU			(202)	2-0:	1-09 17:16:33)		

Или конкретный модуль всех агентов с инвентарем, выбрав модуль и нажав на Search.

Group	All	•	Module	deo 💌	Saurth O
Agent	All C		Search		Search Q
Date	Last 💌		Order by 🗌 agent		
					Export this list to CSV .a,
Video		(2	022-01-06 13:57:48))	
Agent	Controller	Mode	I	Company	Timestamp
munchkin_agent	GD 5446	VGA c	ompatible controller	Cirrus Logic	2022-01-09 17:56:32
keep_p	GD 5446	VGA c	ompatible controller	Cirrus Logic	2022-01-09 17:56:33
euclides	QXL paravirtual graphic card	VGA c	ompatible controller	Red Hat, Inc.	2022-01-09 15:32:47

Даты и изменения в инвентаризации

В подробном просмотре инвентаризации агента с помощью селектора можно выбрать дату отображения конкретного отчета об инвентаризации:

Monitoring INVENTORY



Если вы заметили, что даты отсутствуют, это, вероятно, потому, что в данные не изменились после последнего выполнения инвентаризации. То есть, Pandora FMS сохраняет данные инвентаризации только тогда, когда они изменяются после последнего выполнения

Экспорт данных инвентаризации в CSV

Через Monitoring → Inventory можно экспортировать данные инвентаризации, полученные в результате фильтрации, в CSV-файл.

Выберите фильтр и, когда данные будут доступны, выберите Export this list to CSV.

Monitorin	g ORY					
Group Agent	All		•	Module Search	RAM	Search Q
Date	Last	•		Order by agent		
						Export this list to CSV ,a,
RAM		((2022	2-01-09 12:	08:11)	
Agent		Model		Size		Timestamp
munchkin_agent		System Memory		4092MiB		2022-01-09 18:12:32
		DIMM RAM		4092M	іВ	2022-01-09 18:12:32

Создается файл с данными инвентаризации, разделенные точкой с запятой.

Различия между версиями инвентаризации

Режим блоков

В версии Pandora 5.1 можно наглядно показать различия между двумя конфигурациями, отображая их в двух колонках, чтобы увидеть разницу. Режим блоков указывает, что результатом модуля инвентаризации является один элемент, а не интерпретирует каждую строку как различные элементы одного типа, как это было сделано в модулях инвентаризации, рассмотренных выше.

Блочный режим настраивается (Block mode) при определении локального или удаленного модуля инвентаризации:

Name	NIC
Description	Network Interface Cards
OS	Windows
Interpreter	/usr/bin/perl (i)
Block mode	
Format (j)	Caption;MACAddress;IPAddress

Когда модуль настроен в блочном режиме, он позволяет просматривать его по секциям(для визуального наблюдения за изменениями).

Module NIC V Date Now V	Search Diff view		Search 🗮
NIC - (January 9, 2022, 7:08 am)	I	MACAddress	IDAddress
Intel(R) 82579LM Gigabit Network Connection:44:37:E6:40:	F:EA:192.168.1.47	MACAUULESS	IFAULIESS

Представление в виде двух колонок показывает различия между одной версией инвентаризации и другой, и вы даже можете выбрать версию по дате.

Monitoring / View / Inventory KEPLER		>	(i-)		X	Ŧ	٠	-	¥	۰	۲	*
2022-01-09 12:08:11 * 1 Intel(R) 82579LM Gigabit Network Connection:44:37:E6:AC:4F:EA:192.168:1.47 2	NK Pr	1 2	Intel(R) 8: SAMSUN	2579LM (G Mobile	Gigabit N USB Ren	etwork C note NDIS	onnectio	n:: k Device	(02:34:60	22-01-09 D:72:74:	9 13:43:0 7A;192:1	68.192.3
		3										

генерируется событие.

events 🕐			40	,a,	٣	Ŧ	ж	#
> Filter								
Current filter Not set. Event status Duplicated Group events Show 20 entries	Not validated.	Max. hours old	Last 8	hours.		Previ	ous 1	2 Next
S. Event name	Agent ID	s v Timestamp	Event Id	Comment	Opti	ons		
Configuration change: DELETED RECORD: Intel(R) 82579LM Gigabit Network Connection;44:37:E6:AC:4F:EA;192.168.1.47 NEW RECORD: Int Connection;; SAMSUNG Mobile USB Remote NDIS Network Device;02:34:6D:72:74:7A;192.168.192.3 for agent 'KEPLER' module 'NIC'.	43 🔸	34 minutes 10 seconds #4	84749		0	~ I	1	
recovered (Critical condition) assigned to (Host Alive)	1 対	38 minutes 45 seconds #4	84745		Q	~ I	1	
recovered (Critical condition) assigned to (Host Alive)	15 対	38 minutes 45 seconds #	84747		Q	~ 1	1	
Module 'Service Netlogon - Status' is going to CRITICAL (0)	43 🔸	39 minutes 10 seconds #4	84742		ଷ୍	~ 1	1	

Предупреждения инвентаризации

Версия 751 NG или позже.

Предупреждения инвентаризации используются для запуска конкретных предупреждений о содержимом инвентаря группы агентов. Как и предупреждения SNMP или предупреждения о событиях, они не применяются агентом к агенту, а являются глобальными, в данном случае они применяются группами.

Чтобы установить их, необходимо перейти в раздел Alerts \rightarrow Inventory alerts.

*	Tools	
A	Discovery	
۲	Resources	List of Alerts
٤	Profiles	Templates
∢	Configuration	Actions
۰	Alerts	Commands
Ş.	Events	List of special days
Ē	Servers	Alert correlation
*	Setup	SNMP alerts
Τī	Admin tools	Inventory alerts
d-D	Links	
۲	Update manager	
ıî۱	Module library	
		Pandora FMS v7.0NG.759 - OUM 759 - MR 51
		Page generated on 2022-01-09 14:52:38

Предупреждения инвентаризации имеют поля, аналогичные другим предупреждениям, такие как имя, описание, *временной порог* и действие, как указано в главе о предупреждениях Pandora FMS. Здесь объяснены их различия./p>

- Группа в данном случае действует как условие предупреждения, так что предупреждения будут оцениваться для любых данных, поступающих от агента этой группы.
- Эти предупреждения также имеют опцию деактивировать событие, чтобы при срабатывании предупреждения не генерировалось событие предупреждения. Это полезно, так как возможно, что при применении инвентаризационных оповещений многие предупреждения могут срабатывать или включаться за одно выполнение.

Условие срабатывания предупреждения



Предупреждения об инвентаризации оцениваются в трех различных режимах: сопоставление строк, разрешенный список и ограниченный список.

Сопоставление текстовых строк

В этом режиме, если определенная строка поступает в определенный модуль инвентаризации, например, "software", срабатывает установленное действие. Следует отметить, что модули инвентаризации имеют динамические поля; т.е. в модуле инвентаризации программного обеспечения есть поле имени, версия и описание:

serpentis	acl	2.2.51	Access control list utilities
	aic94xx-firmware	30	Adaptec SAS 44300, 48300, 58300 Sequencer Firmware for AIC94xx driver
	alsa-firmware	1.0.28	Firmware for several ALSA-supported sound cards
	alsa-lib	1.1.6	The Advanced Linux Sound Architecture (ALSA) library
	alsa-tools-firmware	1.1.0	ALSA tools for uploading firmware to some soundcards
	apr	1.4.8	Apache Portable Runtime library
	apr-util	1.5.2	Apache Portable Runtime Utility library
	atk	2.28.1	Interfaces for accessibility support

Таким образом, вы можете установить предупреждение для любого из трех динамических полей. Это идеальный вариант, если вы ищете конкретный пакет или пакет определенной версии:

Inventory modules	Software (Linux)	~
Condition	Match 🗸	
	Name	
	Version	
	Description	

Будут отображены все поля модуля инвентаризации. В этих полях вы можете использовать регулярные выражения для более сложного поиска. Если поле оставлено пустым, оно считается .* (оно покажет *match* или будет совпадать с любым значением).

Ограниченный список

В этом случае вы должны указать только одно поле типа модуль инвентаризации и задать список строк (по одной на строку), чтобы, если агент содержит элемент из этого списка, сработало оповещение. Например, в случае программного обеспечения, этот ограниченный список (Black list) - это список пакетов программ, которые не должны быть установлены на машине. Если на машине установлен один из этих пакетов, сработает предупреждение.

Inventory modules	product_key (Windows)
Condition	Black list 🖌
	Key 🗸
	347637433473647364 234723646732467536 234736453653652643 374374364563545612

Разрешенный список

Действует так же, как и в предыдущем случае. Укажите список элементов для одного из полей инвентаризации; однако, этом случае значение модуля инвентаризации должно всегда находиться в одном из элементов списка, *иначе сработает предупреждение*.

Inventory modules	Users (Windows)	~
Condition	White list 🗸	
	User 🖌	
	Artica Admin Administrator	

Использование предупреждений инвентаризации



Эта функция действительно полезна для обнаружения уязвимых версий устройств, неавторизованных пользователей на машинах или неавторизованного программного обеспечения на компьютерах.

Вернуться в оглавление Документации Pandora FMS