Files (pre v2)

- Introduction
- How does it Work?
- Creating File Entries
- Viewing File Details
- Enabling the Feature Under Windows
- API / Web Access?
 - API Routes
 - Web Application Routes

Introduction

As at version 1.12.8, Open-AudIT can now retrieve details about a file or directory of files and monitor these files for changes as per other attributes in the Open-AudIT database.

This feature works out of the box for Linux Open-AudIT servers, but needs a change to the service account name under a Windows Open-AudIT server.

Supported clients are Windows and Linux.

How does it Work?

When a device is Discovered the audit script will be injected with the file (or directory) details. Both audit_linux.sh and audit_windows.vbs will be populated, regardless of the file path. If you're thinking "but putting a Linux path into a Windows machine will break things!", it won't break, you just won't receive any data from that file or directory entry.

Retrieved details will be stored in the "file" database table and are stored like any other attribute. File details will be stored as any other attribute and generate alerts if any of the following attributes change - 'full_name', 'hash', 'inode', 'last_changed'. The table contain a system_id, first_seen, last_seen and current columns as well as the file details.

Attributes recorded are:

Windows - name, size, directory, SHA1 hash (of the file contents), last changed, permissions, owner, version (file permitting).

Linux - name, size, directory, SHA1 hash (of the file contents), last changed, meta data last changed, permissions, owner, group, inode.

You will see a section in both the Windows and Linux audit scripts as below:

```
# DO NOT REMOVE THE LINE BELOW
# Configuration from web UI here
```

Below these lines are where the variables are injected into the script. Following on from our earlier example, the Linux audit script is populated with our directory like so:

```
# DO NOT REMOVE THE LINE BELOW
# Configuration from web UI here
files[1]="/etc/init.d/"
```

The audit script will use the files[] array and retrieve the file details.

If you would like to use the script outside of Discovery we have created another endpoint called "scripts". See the documentation here - Scripts.

Creating File Entries

To create an entry to track either a single file or a directory of files, use Open-AudIT Enterprise and go to menu -> Views -> Files and click the Create button.



Create a file by providing values for the path (either the file or a directory with a trailing slash) and an optional description. Click Submit.

2000.016	and other states	5. 1041. MP.	
1.4	t ward		
	- faile feet		
1.000			
1.114			
	MV.		
			-

Once you have created the file you will see it appear in the list at menu -> Views -> Files.



An entry will be create in the Open-AudIT database, in the "files" table.

Viewing File Details

File details will appear under the "Settings" menu item for a device. They are displayed as below. This is from a Linux machine using our /etc/init.d/ entry from earlier.



The database entry will look as below (for a single file).

```
id: 48
        system_id: 8
          current: y
       first_seen: 2016-08-04 00:56:35
        last_seen: 2016-08-04 00:56:35
         files_id: NULL
             name: single
        full_name: /etc/init.d/single
             size: 590
        directory: /etc/init.d
             hash: 27579d05edbd1b71307d2059a6c3370a00823c54
     last_changed: 2014-03-13 11:33:14
meta_last_changed: 2014-08-22 17:42:38
       permission: 755
            owner: root
            group: root
             type:
          version:
            inode: 5374232
```

Enabling the Feature Under Windows

There is no need to do anything if you're running Open-AudIT on a Linux server.

Windows clients are just fine and require no special actions, however.... to enable this feature the audit script must be run locally on the target Windows system. It cannot be run remotely as we do with WMI calls when running the audit script on one Windows machine, while targeting a second Windows machine. To do this we need to copy the audit script to the target Windows machine and then run it. Unfortunately the service account that Apache runs under is the Local System account. This account has no access to remote (network based) resources. To work around this issue the service must be run under another account. It is easiest to just use the local Administrator account, but you can try any account you like as long as it has the required privileges. The Local System account has as much local access as the local Administrator account.

Navigate to the Service list.

mind.	G hereitad		
	Spanland .	have - buckets inter	timeter lighter
	the formula	Contract Contract	hand and have
	(min) for marine	Contractor Instance	hand being
		Contration Informed	the state of the s
	(month)	Contractory on the Decide to	Terral Andrews
	Admitted 3 statistics in	Contractor Sector -	Intel Intellige
	NO. 187.2 P 20120-1-1-8	Column Carbon Statements	Design (Married)
	and the second sec	Chairman high Tanakad Incide	A strength of the strength of the
	1	Starbusters fatan's tate	Anna maintain
		Annal Street, Instant, Spin-	hand with the
		Contraction Contract.	Tabled Intelligence
		Brithford later handshi linder	Annual International
		Supplemented Second Incide	land and being
	1	Computer Woman Property L.	INSPI UNIVERSITY
		Control Server Provide La	hand uniform
		Company to be build by light	Advert Wood 1
		Complete here failed and	Address and hope
	1	Desprivation, Portlel, Kalad	Antel Allebe
	1	Cottoe Insteau Inste	Advanta institution
		Charach Maria, Pallana, Jacket	Advert D., Low Service
		Contracts by contracts of the fiber of	formed and for one
	1	Report futer	New workship
	1	Childrente Southalb	Nexal Intelligence
		Contractor Tel. Person L. David	Adverte institutes
		Garballum, Indus, Indu	Anna R. Model.
		Cashing Indial States	

Double click the apache 2.2 service.

	Antibility Antibility (Constrained States)	Security and a second s
	Andrew Barris Barr	Next Active Next A
	Construction of the second secon	No. 2019 No. 2019 No. 2019 No. 2019 No. 2019 No. 2019 No. 2019 No. 2019 No. 2019
	The finance intervention of the second of th	New order Text of the second s
	Image: Table 11 to 000 to	Tend APT - A
Reserved and the second	March 1997 The American Strength and Strengt	Subal Solution
Marchine Mar	The second secon	Solid Model Server D., Lawlord
	Tell à la contente de la contente la contente de la	Address D
	V valadit particul (19) par e la valazione Nelle sport Manza este la valazione della valazione Secondata Sand Secondata Sand Secondata della valazione della valazione della valazione Nelle valazione della valazione della valazione della valazione Nelle valazione della valazione della valazione della valazione Nelle valazione della valazione della valazione della valazione della valazione della valazione della valazione Nelle valazione della v	Anna Anna
	Nera Sec. Juneau 2 Hit is a crime same data adm. December 2 Ben Proc. Procession	
Normal and Array	No new first series and a series. Decomes Series Series Base Press Press and Press and Press P	time instant
The market area and another. A set of the se	Notes or final active of the orders Device and Dated Date: Date: Proc. Procession	Pand Laplace
Decama Jand Decama Ja	Designation Termination Termination Termination	TARK INCOM
Decause Joint Decause Joint Decause Joint Control Dec	Decoma Serial	101.4 LODVA
Are the the the the the the the the the th	Der De Pex Pour	
Constraints Constrain		
Construction and the and and the part of the series Construction and the series and the part of the series Construction and the series and the series Construction and the series and the series Construction and the series and the series	Name and its as an annual to say the say of the say of the says	and a second sec
Arrest Argenetics The formed for the formed for t		hand inches
Arrent Landon	50/55	and a local section.
	bearing [Annal (
		internal landleri
OR Genet And Market Market		Tend tealings
	and see a second second	tional income
		Address and the

Click the tab for logon and then click the "this account" option. You might want to click the Browse button and search for the account. Click OK and then restart the service.



Apache will now be running under an account with network access and Open-AudIT will now be able to copy the audit script to the target Windows machine and run it, hence retrieving file details.

API / Web Access?

You can access the /files collection using the normal Open-AudIT JSON based API. Just like any other collection. Please see the API documentation for further details.

API Routes

Request Method	ID	Action	Resulting Function	URL Example	Notes	Example Response
GET	n		collection	/files	Returns a list of files.	files_collection.json
GET	у		read	/files/{id}	Returns a file's details.	files_read.json
PATCH	У		update	/files/{id}	Update an attribute of a file entry.	files_patch.json
POST	n		create	/files	Insert a new file entry.	files_create.json
DELETE	у		delete	/files/{id}	Delete a file entry.	files_delete.json

Web Application Routes

Only available under Open-AudIT Enterprise

Request Method	ID	Action	Resulting Function	URL Example	Notes
GET	n	create	create_form	/files/create	Displays a standard web form for submission to POST /files.
GET	У	update	update_form	/files/{id}/update	Show the script details with the option to update attributes using PATCH to /files/ $\{id\}$