Files

Introduction

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:

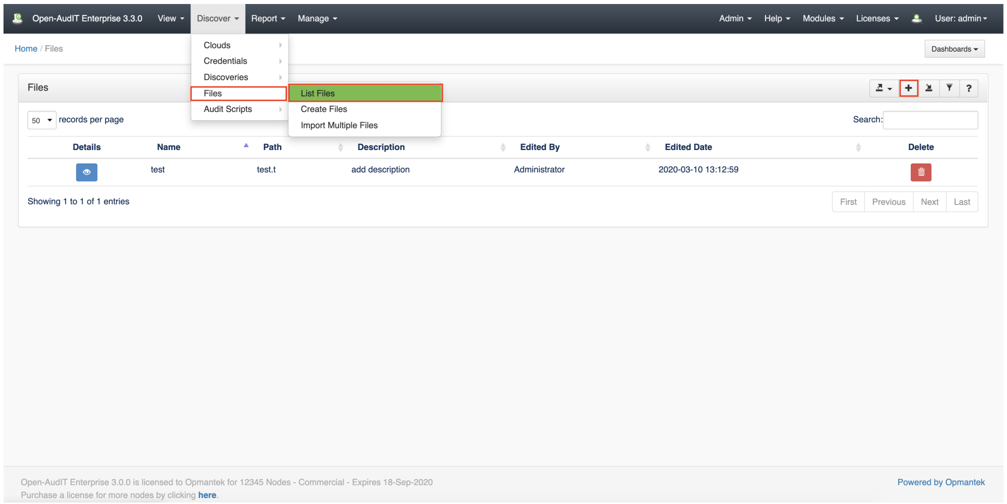
```
# DO NOT REMOVE THE LINE BELOW
# Configuration from web UI here
files[1]="/etc/init.d/"
```

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

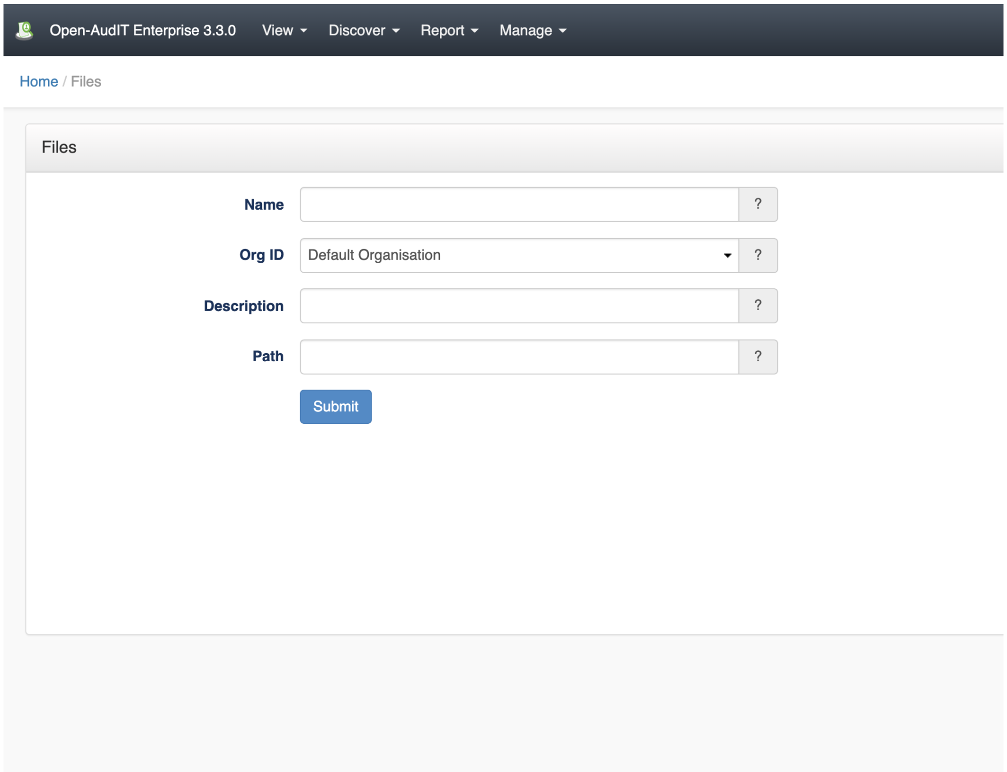
To create an entry to track either a single file or a directory of files, use Open-AudIT Enterprise and go to menu: Discover-> Files -> Create Files. Create a file by providing values for the path (either the file or a directory with a trailing slash) and an optional description. Click Submit. Once you have created the file you will see it appear in the list at Discover -> Files -> List Files.



Details	Name	Path	Description	Edited By	Edited Date	Delete
👁	test	test.t	add description	Administrator	2020-03-10 13:12:59	🗑

Showing 1 to 1 of 1 entries

Open-AudIT Enterprise 3.0.0 is licensed to Opmantek for 12345 Nodes - Commercial - Expires 18-Sep-2020
Purchase a license for more nodes by clicking here.



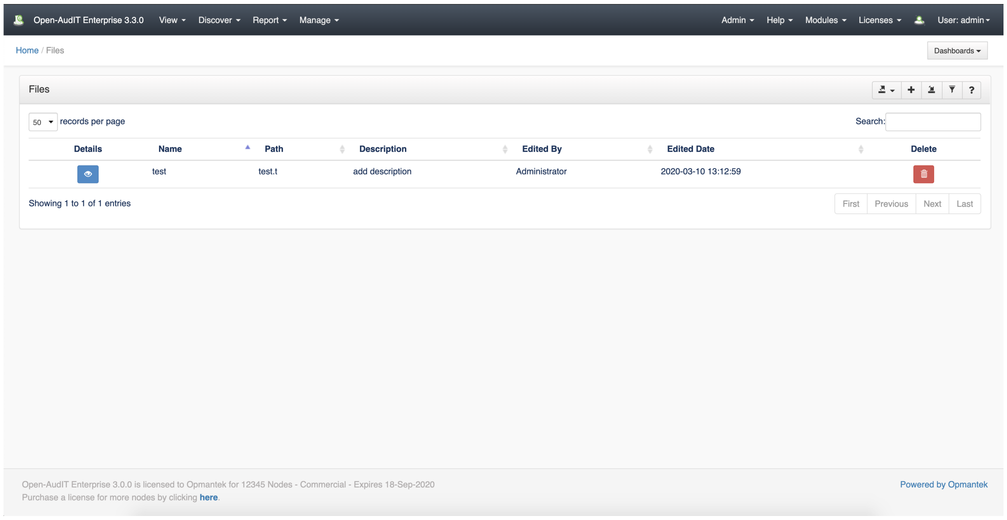
Name	
Org ID	Default Organisation
Description	
Path	

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

Viewing File Details

Go to menu: Discover -> Files -> List Files.

You will see a list of files. You can view a file by clicking on the blue view icon. You can also edit or delete your file.



Files

50 records per page

Search:

Details	Name	Path	Description	Edited By	Edited Date	Delete
	test	test.t	add description	Administrator	2020-03-10 13:12:59	

Showing 1 to 1 of 1 entries

First Previous Next Last

Open-AudIT Enterprise 3.0.0 is licensed to Opmantek for 12345 Nodes - Commercial - Expires 18-Sep-2020
Purchase a license for more nodes by clicking **here**.

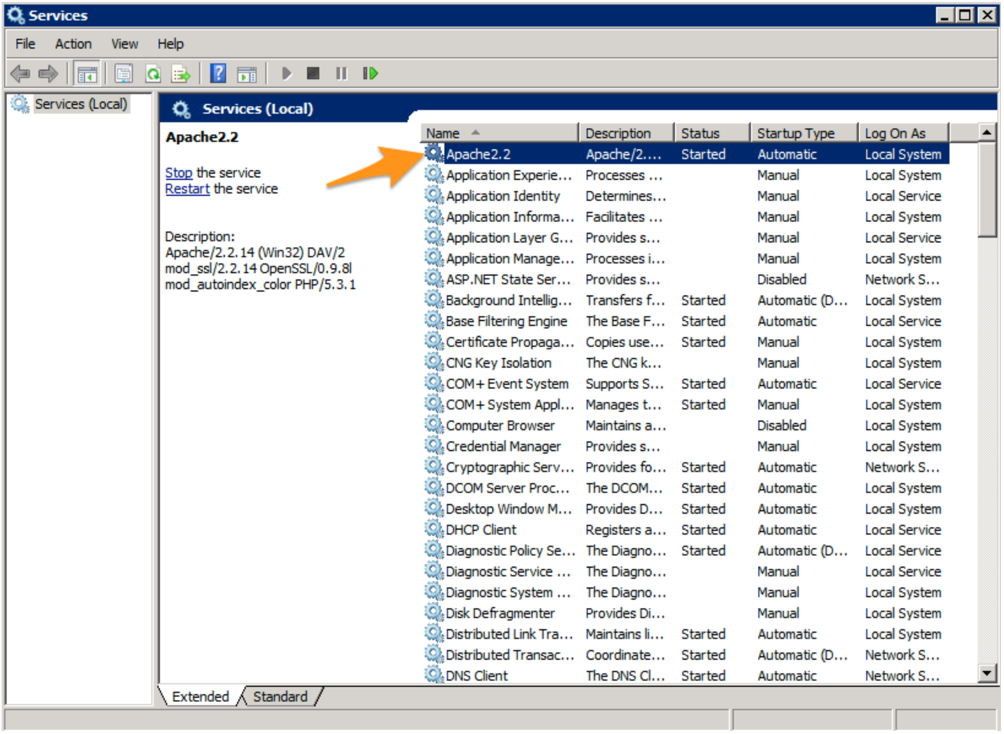
Powered by Opmantek

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.



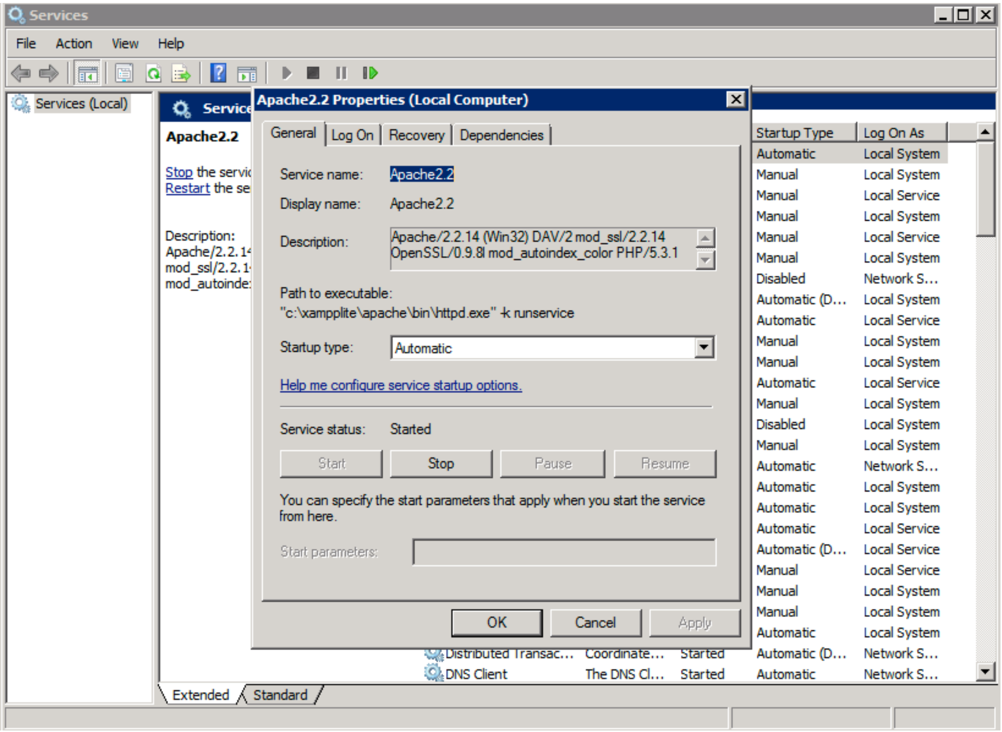
Apache2.2

Stop the service
Restart the service

Description:
Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color PHP/5.3.1

Name	Description	Status	Startup Type	Log On As
Apache2.2	Apache/2....	Started	Automatic	Local System
Application Experie...	Processes ...		Manual	Local System
Application Identity	Determines...		Manual	Local Service
Application Informa...	Facilitates ...		Manual	Local System
Application Layer G...	Provides s...		Manual	Local Service
Application Manage...	Processes i...		Manual	Local System
ASP.NET State Ser...	Provides s...		Disabled	Network S...
Background Intellig...	Transfers f...	Started	Automatic (D...	Local System
Base Filtering Engine	The Base F...	Started	Automatic	Local Service
Certificate Propaga...	Copies use...	Started	Manual	Local System
CNG Key Isolation	The CNG k...		Manual	Local System
COM+ Event System	Supports S...	Started	Automatic	Local Service
COM+ System Appl...	Manages t...	Started	Manual	Local System
Computer Browser	Maintains a...		Disabled	Local System
Credential Manager	Provides s...		Manual	Local System
Cryptographic Serv...	Provides fo...	Started	Automatic	Network S...
DCOM Server Proc...	The DCOM...	Started	Automatic	Local System
Desktop Window M...	Provides D...	Started	Automatic	Local System
DHCP Client	Registers a...	Started	Automatic	Local Service
Diagnostic Policy Se...	The Diagno...	Started	Automatic (D...	Local Service
Diagnostic Service ...	The Diagno...		Manual	Local Service
Diagnostic System ...	The Diagno...		Manual	Local System
Disk Defragmenter	Provides Di...		Manual	Local System
Distributed Link Tra...	Maintains li...	Started	Automatic	Local System
Distributed Transac...	Coordinate...	Started	Automatic (D...	Network S...
DNS Client	The DNS Cl...	Started	Automatic	Network S...

Double click the apache 2.2 service.



Service name: Apache2.2

Display name: Apache2.2

Description: Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color PHP/5.3.1

Path to executable:
"c:\xampplite\apache\bin\httpd.exe" -k runservice

Startup type: Automatic

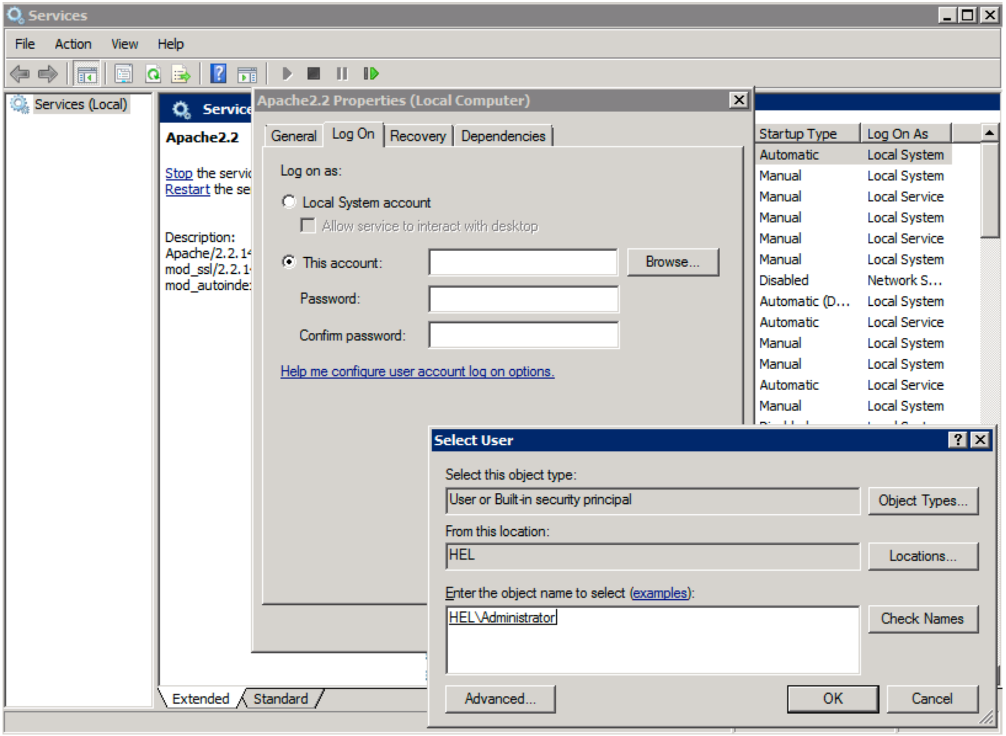
Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

			Startup Type	Log On As
			Automatic	Local System
			Manual	Local System
			Manual	Local Service
			Manual	Local System
			Manual	Local Service
			Manual	Local System
			Disabled	Network S...
			Automatic (D...	Local System
			Automatic	Local Service
			Manual	Local System
			Manual	Local System
			Automatic	Local Service
			Manual	Local System
			Disabled	Local System
			Manual	Local System
			Automatic	Network S...
			Automatic	Local System
			Automatic	Local System
			Automatic	Local Service
			Automatic (D...	Local Service
			Manual	Local Service
			Manual	Local System
			Manual	Local System
			Automatic	Local System
Distributed Transac...	Coordinate...	Started	Automatic (D...	Network S...
DNS Client	The DNS Cl...	Started	Automatic	Network S...

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.



Log on as:

○ Local System account

□ Allow service to interact with desktop

● This account:

Password:

Confirm password:

Select this object type:
User or Built-in security principal

From this location:
HEL

Enter the object name to select (examples):
HEL\Administrator

Startup Type	Log On As
Automatic	Local System
Manual	Local System
Manual	Local Service
Manual	Local System
Manual	Local Service
Manual	Local System
Disabled	Network S...
Automatic (D...	Local System
Automatic	Local Service
Manual	Local System
Manual	Local System
Automatic	Local Service
Manual	Local System

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.

Database Schema

The database schema can be found in the application is the user has database::read permission by going to menu: Admin -> Database -> List Tables, then clicking on the details button for the table.

API / Web Access

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