Changes

Introduction

Open-AudIT has a powerful change detection engine. Any device attributes that are added, removed or changed will be detected and stored. These changes can be reported upon and the relevant data confirmed as to what was expected from your company change and release process.

When a device is audited, attributes are divided into sections which correspond to tables in the database.

Each device (computer, router, printer, et al) has an entry in the "~~system~~" (devices as at 5.0.0) table. Each entry in the "devices" table has an "id" column. This value is unique - it is an auto-incrementing id.

When the audit result is processed, each item in each section has its audit result compared to what is in the database.

For each section, if the key columns (see below table) contain the identical values, it is considered already installed and has its 'last_seen' attribute updated. No change_log entry is created.

If any of the key columns do not match, it is considered a new attribute and is inserted. A change_log entry is created if the device had other attributes already present in the table.

At the completion of the audit processing, any database items that have not been updated (or inserted) are considered to not be present. The 'current' attribute for this item is set to 'n' and a change_log entry is generated.

So, we can determine if something is currently installed - the current column is 'y'.

We can determine when something was initially detected - the "first_seen".

We can determine if something was installed after the initial audit - first seen will be different in the component and device tables.

We can determine if something is not currently installed, but previously was - current = 'n'.

We can determine the last time we detected an item - last_seen.

At any given point, we can determine what was on a system - by using the audit_log table and selecting the relevant components based on first_seen and last_seen.

Each section and its matching key columns are below.

NOTE - There are some exceptions as detailed below.

*1 - If the computer is a VMware Esx machine it also uses the net_index and connection columns.

*2 - If the computer is an AIX machine, we use the partition name.

Table	*Attribute #1*	*Attribute #2*	*Attribute #3*	*Attribute #4*	*Attribute #5*
bios	description	manufacturer	serial	smversion	version
disk	model	serial	hard_drive_index	size	
dns	ip	name	fqdn		
file	full_name	hash	inode	last_changed	
log	name	file_name	overwrite		
memory	bank	size	serial		
module	description	module_index	serial		
monitor	model	manufacturer	serial		
motherboard	model	manufacturer	serial		
netstat	protocol	ip	port	program	
network *1	mac				
ip	ip	mac	netmask		
optical	model	mount_point			
pagefile	name	initial_size	max_size		

partition *2	name	hard_drive_index	mount_point	size	
print_queue	device				
processor	description				
route	destination	next_hop			
san	serial				
scsi	model	manufacturer	device		
server	name	type	full_name	version	
server_item	name	type	instance		
service	description	name	executable		
share	name	path			
software	name	version			
software_key	name	string	rel	edition	
sound	model	manufacturer			
task	name	task			
user	name	sid			
user_group	name	sid			
variable	program	name	value		
video	model				
vm	name	uuid			
windows	service_pack	build_number			