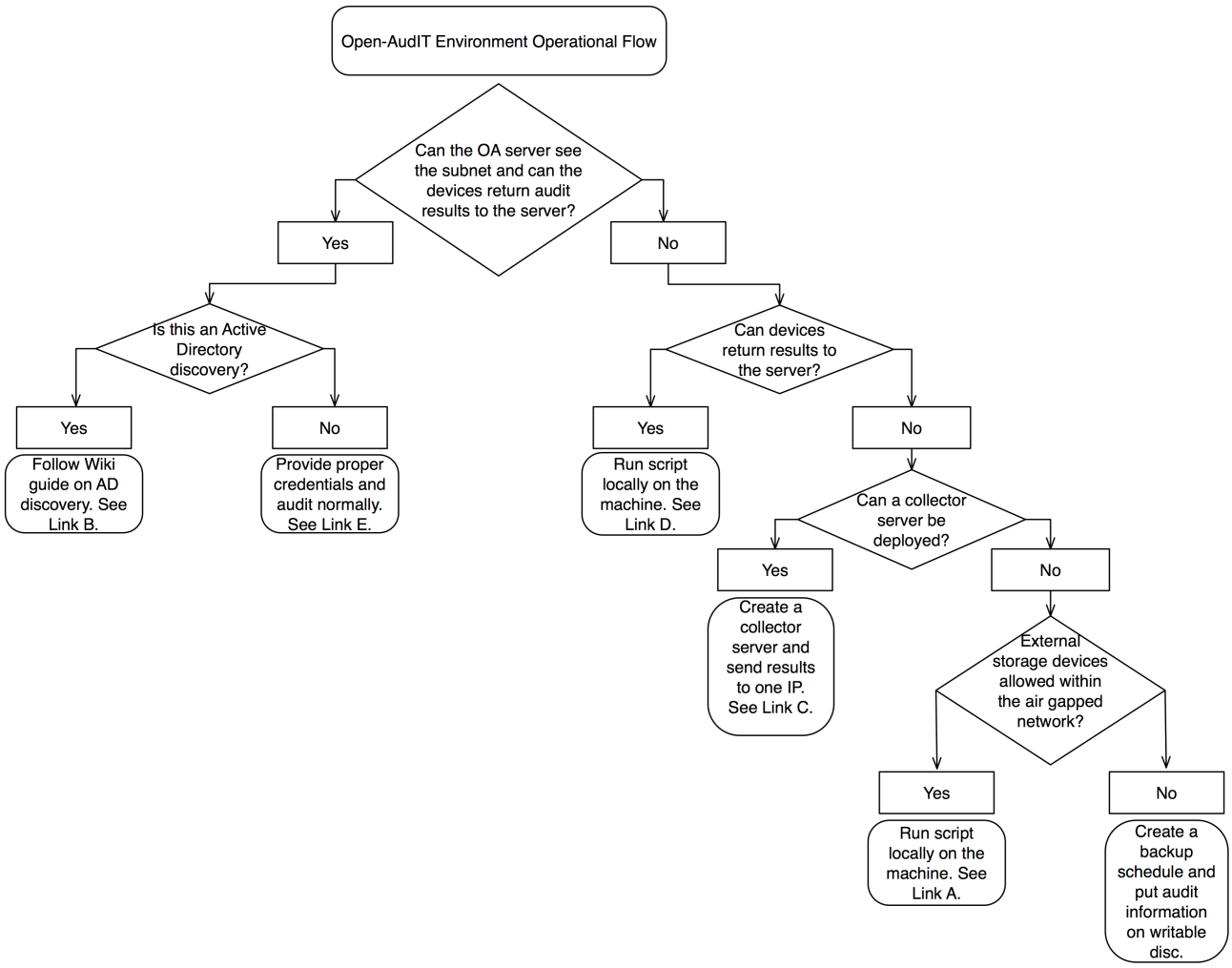
How to Audit in complex network environments

- Auditing with a script
- Computer with no network connectivity to the Open-AudIT server.
- Computer not on the domain.
- Active Directory discovery
- Other Commands
- Other helpful resources

Every environment is different and we understand that. We are often questioned if Open-AudIT is pcidss compliant, can audit in a DMZ (demilitarized zone) or an air gapped network. The answer to all of these questions is yes however, it is a matter of process. This How-To is designed to help you think through this process and assist in implementing Open-AudIT into a variety of complex network environments. Follow the chart and decide which audit methods are most relevant to you and your team and see instructions below on how to accomplish these complex audits.



Link A - Audit a computer with no network connectivity

Link B - How to use Active Directory Discovery

Link C - Collector / Server

Link D - Auditing with a Script

Link E - Building your Network Discovery

Auditing with a script

Open-AudIT can perform audits simply with the proper credential set of a device or subnet. In some cases there may be no internet access or it is a remote machine, etc. this is when auditing using a script can come in handy.

Auditing using a script (Windows)

Wiki resource - How to audit a Computer#Auditingusingascript(Windows)

Assuming you have an XAMPPLite install of Open-AudIT on a Microsoft Windows machine.

Copy the file c:\xampplite\open-audit\other\audit_windows.vbs to a suitable location. Do **not** remove this file from it's original location as it is needed by the web interface.

Open your copy of audit_windows.vbs in a text editor. Check the following variables are set as below:

- submit_online = "y"
- create_file = "n"
- url = "http://YOUR_SERVER/open-audit/index.php/input/devices"
- debugging = "3"

Open a command prompt and run the script with ***cscript audit_windows.vbs***. *Do not double click the script to run it as this will use wscript instead of cscript and spawn many popup windows.*

It should run and post the result to the database. Go back to your web browser and load Open-AudIT. You should have a group or two created. Go into one of them and click the machine name. You should see the machine details.

NOTE - To prevent any output to the command window you can set debugging = "0" and run the script with ***cscript //nologo audit_windows.vbs .***

Auditing using a script (Linux / SSH)

Wiki resource - How to audit a Computer#Auditingusingascript(Linux/SSH)

We have unix based (bash. ksh, etc) scripts for Linux, AIX, OSX, Solaris computers.

To use the Unix audit script located at open-audit/other/audit_linux.sh:

- Edit the script and ensure the $url variable is set to your webserver - the same as is done for the audit_windows.vbs script.
- Copy it to the target computer.
- Ensure the script has permission to operate (chmod 777 audit_linux.sh is fine).
- Run the script with root level permission either by sudo or directly as root.

The script has variables that can be set the same as the variables in audit_windows.vbs. You could (for example) dynamically set the $url variable when you run the script by

```
./audit_linux.sh url=http://your_server/open-audit/index.php/input/devices
```

The variables that are accepted on the command line are:

submit_online - Defaults to "n". If set to "y" it will submit the audit result to the URL as specified by the url variable.

create_file - Defaults to "y". If set to "y", an XML file will be created and saved as per the audit_windows.vbs script. This file can be manually copied and submitted to the server at a later stage if desired.

Computer with no network connectivity to the Open-AudIT server.

Not every Windows computer will be a simple domain connected machine. Sometimes you may have a server in a DMZ with no network connectivity to the internal network, a machine not on a domain, a standalone machine not networked at all, etc. There are various options to overcome these.

Copy the audit script to a USB drive, go to the remote computer and insert the USB drive. Open a command prompt and navigate to where you copied the script. Run the script and output to an XML file using the command

```
cscript audit_windows strcomputer=. submit_online=n create_file=y
```

An XML file named COMPUTERNAME_DATE.xml should be created. Close the terminal window. Remove the USB drive and go to a computer with Open-AudIT connectivity. Open the XML file and copy the XML and log in to the Open-AudIT web application and go to menu -> Manage -> Devices -> Create Devices. You will see options for manually copying and pasting the file contents or uploading the file directly.

Computer not on the domain.

If you can see the computer on the network and it has it's firewall opened to allow remote WMI/VBscript, you can run the audit script using the remote credentials.

```
cscript audit_windows.vbs strcomputer=REMOTE_COMPUTER_NAME struser=REMOTE_DOMAIN/REMOTE_USERNAME
strpass=REMOTE_PASSWORD
```

You may need to substitute the string "workgroup" or the remote computer name for REMOTE_DOMAIN above.

Active Directory discovery

How to use Active Directory Discovery

Other Commands

This command will run the audit on the local PC and output the results to a file (in the current directory). The "." can be used in place of the local machine name:

```
cscript audit_windows.vbs . submit_online=n create_file=y
```

Other helpful resources

What Operating Systems will the audit scripts run on?

How to audit a Computer

How to audit a subnet using a script

Configuring Open-Audit with HTTPS/SSL

Information about how to get data into Open-AudIT