

XenServer Auditing Tool Readme

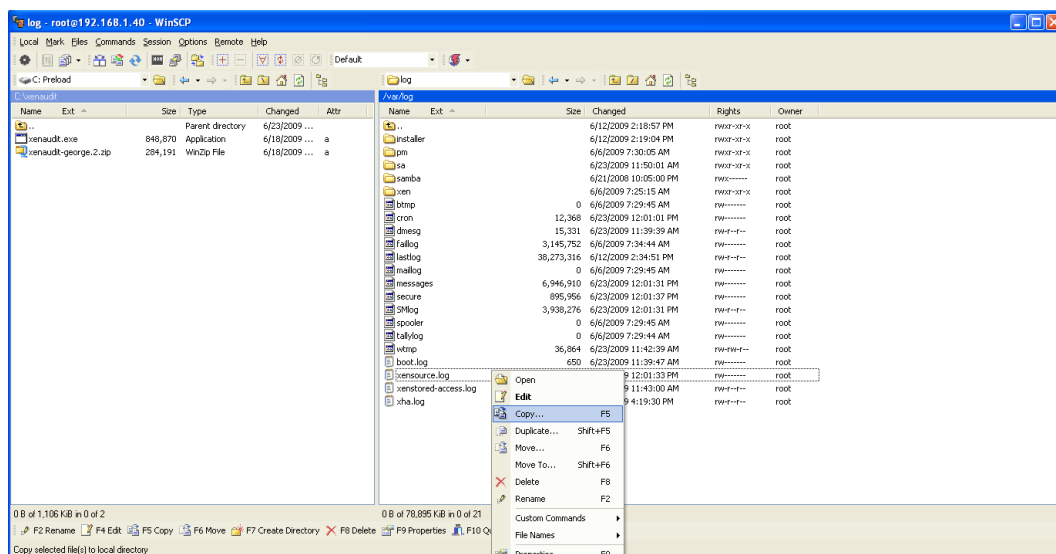
Using the XenServer Auditing Tool

Download the auditing tool from the Citrix XenServer Resource Kit [page](#) and extract the xenaudit.exe file from the xenaudit.zip to a directory on a Windows system, i.e. c:\xenaudit

Step 1 – Copying the log file(s)

Copy the xensource.log file from the XenServer resource pool master server to your Windows system. WinSCP (freely downloadable [here](#) and shown below) is a good GUI-based tool for copying the file. The xensource.log file is accessible in the /var/log directory on the XenServer.

Note: When XenServer log files grow beyond certain filesize, they will be split up in multiple files. Older logging data will be stored in xensource.log.1, xensource.log.2 etc.



Step 2 – Converting the log file(s)

Using the Windows command prompt, run the following command:

xenaudit.exe xensource.log > log.csv

```

C:\WINDOWS\system32\cmd.exe

Directory of C:\xenaudit

06/23/2009  01:30 PM  <DIR>          .
06/23/2009  01:30 PM  <DIR>          ..
06/18/2009  03:20 PM                848,870 xenaudit.exe
06/18/2009  10:22 AM                284,191 xenaudit.zip
06/23/2009  02:27 PM                28,513,488 xensource.log
              3 File(s)                29,646,549 bytes
              2 Dir(s)      102,950,400,000 bytes free

C:\xenaudit>xenaudit.exe xensource.log > log.csv_

```

This will create a comma-delimited administrative log file in CSV format called “log.csv.”

Step 3 – Interpretation of log information

Open the log.csv file using Microsoft Excel, or a similar tool. In Excel, you will see a log similar to what is shown below.

1	date	user name	is local	host name	task name	message
2	20090623 11:08:51.794	joel	FALSE	xenserver5-1	Async.VM.snapshot	task Async.VM.snapshot R:7a37cb3ebf8d (uuid:77f6a238-716d-2a2e-d663-cccbaafc2630)
3	20090623 11:08:51.797	joel	FALSE	xenserver5-1	Async.VM.snapshot	VM.snapshot: Snapshotting VM 'OpaqueRef:aea2d5ae-6e25-e6b4-f5bd-81da66ab47d5'
4	20090623 11:10:48.444	joel	FALSE	xenserver5-1	VBD.destroy	VBD.destroy: Destroying VBD 'OpaqueRef:de08bddd-e2c8-22a9-2bb5-c5fc7bd58b2d'
5	20090623 11:10:48.500	joel	FALSE	xenserver5-1	VDI.destroy	VDI.destroy: Destroying VDI 'OpaqueRef:50d67b95-4970-5f48-f76d-b2f9c9a94695'
6	20090623 11:10:52.964	joel	FALSE	xenserver5-1	VBD.destroy	VBD.destroy: Destroying VBD 'OpaqueRef:6d53223f-46a3-0896-c6df-735591933068'
7	20090623 11:10:53.019	joel	FALSE	xenserver5-1	VDI.destroy	VDI.destroy: Destroying VDI 'OpaqueRef:36caeb35-4de4-72c1-b42b-cdc19d8ca271'
8	20090623 11:12:41.784	joel	FALSE	xenserver5-1	VM.destroy	VM.destroy: destroying VM 'OpaqueRef:e70272fc-117f-338e-403f-fecceb1967ec'
9	20090623 11:12:41.859	joel	FALSE	xenserver5-1	VBD.destroy	VBD.destroy: Destroying VBD 'OpaqueRef:98f8cb04-dc04-f467-b0f3-6781ebb91b25'
10	20090623 11:12:41.914	joel	FALSE	xenserver5-1	VBD.destroy	VBD.destroy: Destroying VBD 'OpaqueRef:34d25835-5401-119d-1028-f706413df6da'
11	20090623 11:12:41.954	joel	FALSE	xenserver5-1	VM.destroy	VM.destroy: destroying VM 'OpaqueRef:aea2d5ae-6e25-e6b4-f5bd-81da66ab47d5'
12	20090623 11:12:42.005	joel	FALSE	xenserver5-1	VBD.destroy	VBD.destroy: Destroying VBD 'OpaqueRef:c2a5250d-0271-ba2f-ae29-f925ee9bb0df'
13	20090623 11:57:19.934	adam	FALSE	xenserver5-1	Async.VM.clone	task Async.VM.clone R:c8bca4aa54d9 (uuid:d4961761-8e24-1438-8928-d690f3e406ec) cre
14	20090623 11:57:19.935	adam	FALSE	xenserver5-1	Async.VM.clone	VM.clone: Cloning VM 'OpaqueRef:1a2841ff-fa09-5014-ca2b-9656eb73deb0' new_name=
15	20090623 11:57:33.103	adam	FALSE	xenserver5-1	VDI.create	VDI.create: Creating VDI named 'New virtual disk'
16	20090623 11:57:33.712	adam	FALSE	xenserver5-1	VBD.create	VBD.create: Creating VBD connecting VM 'OpaqueRef:3f977d87-28db-6c38-0e61-351b92c
17	20090623 11:57:36.794	adam	FALSE	xenserver5-1	VBD.destroy	VBD.destroy: Destroying VBD 'OpaqueRef:002b6ee1-107a-b09d-d687-4c3239829bc'
18	20090623 11:57:36.834	adam	FALSE	xenserver5-1	VDI.destroy	VDI.destroy: Destroying VDI 'OpaqueRef:bdb0851e-78dc-5c85-a7ff-abc0c1c444a4'
19	20090623 11:57:40.674	adam	FALSE	xenserver5-1	VM.destroy	VM.destroy: destroying VM 'OpaqueRef:3f977d87-28db-6c38-0e61-351b92c9d9d6'
20	20090623 11:57:40.738	adam	FALSE	xenserver5-1	VBD.destroy	VBD.destroy: Destroying VBD 'OpaqueRef:73c8cf2b-ea9c-d6eb-ecf5-6dfdfabfa440'

The columns are:

- **Date:** date and timestamp of action. The format is YYYYMMDD and HH:MM:SS.xxx
- **User name:** Active Directory username for administrator that performed the specific action. If the “root” user was used, this column will either list “root” or it will be blank.
- **Is Local Superuser:** If the “root” administrator initiated the action, this will say “TRUE.” If an Active Directory user initiated the action, this will say “FALSE.”
- **Host Name:** This is the name of pool master server at the time the action was undertaken.
- **Task Name.** The associated XenAPI call from the action performed either at the XenServer CLI or via the analogous GUI-based action in XenCenter.
- **Message:** Details on the action performed, including UUID and/or or description where applicable.

In the example above, we can see the administrative actions performed by administrators “joel” and “adam,” including:

At 11:12 on June 23 we see that Joel destroyed a virtual machine (VM.destroy) and its associated virtual block devices (VBD.destroy).

At 11:57 on June 23 we see that Adam created a virtual machine by cloning an existing virtual machine (async.vm.clone, vdi.create, vbd.create), and then deleted it (vm.destroy).

Note: In the Message field, objects are being listed as uuids. The XenServer CLI can be used to determine the friendly-name for those objects, for example, to determine the friendly name for a Virtual Machine you could use the following CLI command:

```
xe vm-list uuid=<uuid as listed in log file> params=name-label
```